UNITED STATES DISTRICT COURT
WESTERN DISTRICT OF TEXAS
AUSTIN DIVISION

Marc Opperman, *et al*.,	§	
for themselves all others	§	
similarly situated,	§	
Plaintiffs,	§	Case No. 1:12-00219-SS
vs.	§	
	§	
Path, Inc., *et al.,*	§	Jury Trial Demanded
Defendants.	§	

PLAINTIFFS' SECOND AMENDED CLASS ACTION COMPLAINT

Plaintiffs, for themselves and all others similarly situated, allege as follows:

INTRODUCTION

1. Plaintiffs purchased iPhones, iPads and iPod touches (collectively, "iDevices") from Apple, with several built in Apps. Plaintiffs obtained Defendants' Apps from Apple's App Store prior to February 2012.

2. Plaintiffs used their iDevices to maintain their private, personal address books. Unbeknownst to Plaintiffs, the Apps made by Defendants stole their iDevice address books by surreptitiously initiating unnoticeable Internet calls with Plaintiffs' iDevices and transmitting their address books to unauthorized persons.

3. While Apple has known about this threat to its customers and their iDevice address books since it launched the Apple Store in 2008, and has repeatedly represented that it polices its App Store to prevent this from occurring, it has not warned or protected consumers from the threat.

4. Apple did not remove these apps from its App Store, inform its users about this conduct, or correct its testing and review process to appropriately remedy the problem.

5. Based on news reports, including a February 15, 2012 NEW YORK TIMES article, the Apps *Foodspotting, Foursquare, Gowalla, Hipster, Instagram, Kik Messenger, Path, Twitter, Yelp!,* and (via Defendant Chillingo's integrated *Crystal* platform) *Angry Birds Classic* and *Cut the Rope* and the companies associated with each of those that were engaged in surreptitiously transmitting iDevice owners' private, personal address book materials to unapproved recipients Apps. Each did this to various Plaintiffs and similarly impaired their iDevices in this manner.

6. Defendants Hipster and Path publicly admitted that their actions were wrong and apologized. While the remaining Defendants have not followed suit, they, too, are at fault for their unauthorized surreptitious uploads and storage of consumers' address books.

7. As these Defendants, with Apple's approval and assistance, wrongfully used Plaintiffs' iDevices, obtained, invaded and exposed Plaintiffs' private address books, and de-privatized some of the most personal, private and valuable materials that Plaintiffs maintain on their iDevices, Plaintiffs seek damages, as well as declaratory, injunctive, and equitable relief for themselves and all similarly situated persons.

PARTIES

Plaintiffs

8. ***Plaintiff Alan Beuershasen*** resides in Austin, Texas. Mr. Berchausen owns and regularly uses an iPhone with the following Apps: *Twitter, Gowalla, Foursquare* and *Angry Birds Classic*. Mr. Beuershasen acquired each of the identified Apps prior to February 2012.

9. ***Plaintiff Giuli Biondi*** ("Ms. Biondi") resided in Austin, Texas. Ms. Biondi owns and regularly uses an iPhone with the following Apps: *Instagram, Twitter, Yelp!* and *Cut the Rope*.

10. ***Plaintiff Steve Dean*** resides in Austin, Texas. Mr. Dean owns and regularly uses an iPhone with the following Apps: *Twitter, Gowalla* and *Angry Birds Classic*.

11. ***Plaintiff Stephanie Dennis-Cooley*** resides in Virginia. Ms. Dennis-Cooley owns and regularly uses an iPhone and an iPad with following Apps: *Twitter, Kik Messenger, Path* and *Instagram*.

12. ***Plaintiff Claire Hodgins*** resides in Austin, Texas. Ms. Hodgins owns and regularly uses an iPhone with the following Apps: *Twitter, Yelp!, Angry Birds Classic* and *Cut the Rope*.

13. ***Plaintiff Jason Green*** resides in Fayetteville, Arkansas. Mr. Green owns and regularly uses an iPhone with the following Apps: *Instagram, Twitter, Kik Messenger, Path, Angry Birds Classic* and *Cut the Rope*.

14. ***Plaintiff Gentry Hoffman*** resides in Austin, Texas. Mr. Hoffman owns and regularly uses an iPhone with the following Apps: *Twitter, Instagram, Foursquare* and *Yelp!*.

15. ***Plaintiff Rachelle King*** resides in Austin, Texas. Ms. King owns, regularly uses and has regularly used multiple iPhones with the following Apps: *Twitter, FoodSpotting, Hipster, Instagram, Gowalla,* and *Foursquare*.

16. ***Plaintiff Nirali Mandaywala*** resides in Austin, Texas. Ms. Mandaywala owns and regularly uses an iPhone with the following Apps: *Instagram, Twitter, Yelp!, Gowalla, Foursquare, Angry Birds Classic* and *Cut the Rope*.

17. ***Plaintiff Claire Moses*** resides in Austin, Texas. Ms. Moses owns and regularly uses an iPhone with the following Apps: *Twitter* and *Instagram*.

18. ***Plaintiff Marc Opperman*** resides in Austin, Texas. Mr. Opperman owns and regularly uses an iPhone with the following Apps: *Path, Twitter, Instagram* and *Angry Birds Classic*.

19. ***Plaintiff Judy Paul*** resides in Austin, Texas. Ms. Paul owns and regularly uses an iPad and iPhone with the following Apps: *Path, Foursquare, Gowalla, Twitter* and *Yelp!*.

20. ***Plaintiff Theda Sandiford*** resided in Austin, Texas. Ms. Sandiford owns and regularly uses an iPad and iPhone with the following Apps: *Angry Birds Classic, Cut the Rope, FoodSpotting, Foursquare, Gowalla, Instagram* and *Yelp!.*

21. ***Plaintiff Greg Varner*** resides in Austin, Texas. Mr. Varner owns and regularly uses an iPhone with the following Apps: *Twitter, Instagram, Foursquare, Gowalla, Angry Birds Classic* and *Cut the Rope*.

22. Each Plaintiff purchased his or her iDevices prior to February 2012.

23. Each Plaintiff acquired their identified Apps from the App Store prior to February 2012. Each Plaintiff used his or her iDevice(s) and each of these identified Apps while they reportedly were initiating unauthorized address book transmissions and in the manners necessary, as described herein, to trigger the unauthorized taking and upload from his or her iDevice(s) of his or her private address book materials.

Defendants

24. ***Defendant Apple, Inc.*** ("Apple") is a California corporation with offices in Austin, Texas. Apple has appeared in this action.

25. ***Defendant Burbn, Inc.*** ("Burbn"), on information and belief, is a Delaware corporation with its principal place of business at 265 Rivoli Street 4, San Francisco, California 94105. Burbn is not registered to conduct business in Texas and has not designated an agent for service of process. Burbn may be and has already been served by certified mail, return receipt

requested, directed to Burbn at its principal place of business through the Texas Secretary of State as its agent for service of process at Citations Division, 1019 Brazos, Austin, Texas 78701: 265 Rivoli Street 4, San Francisco, California 94105.

26. ***Defendant Chillingo Ltd.*** ("Chillingo") is a United Kingdom limited company with its principal place of business at Beechfield House, Winterton Way, Macclesfield, SK 11 OLP, United Kingdom. Chillingo has appeared in this action.

27. ***Defendant Electronic Arts Inc.*** ("Electronic Arts") is a Delaware corporation with offices in Austin, Texas. Electronic Arts has appeared in this action.

28. ***Defendant Facebook, Inc.*** ("Facebook") is a Delaware corporation with offices in Austin, Texas. Facebook has appeared in this action.

29. ***Defendant Foodspotting, Inc.*** ("Foodspotting") is a Delaware corporation with its principal place of business at 526 2nd Street, San Francisco, California 94107. Foodspotting has appeared in this action.

30. ***Defendant Foursquare Labs, Inc.*** ("Foursquare Labs") is a Delaware corporation with its principal place of business at 36 Cooper Square, 6th Floor, New York, New York. Foursquare Labs has appeared in this action.

31. ***Defendant Gowalla Incorporated*** ("Gowalla") is a Delaware corporation with its principal place of business at 610 W. 5th Street, Suite 604, Austin, Texas 78701. Gowalla has appeared in this action.

32. ***Defendant Hipster, Inc.*** ("Hipster") is a Delaware corporation with its principal place of business at 330 Townsend Street, Ste. 202, San Francisco, California 94107 or 3130 Lowell Ave., California 90032-2913 and its registered Delaware agent for service of process is Agents and Corporations, Inc., 1201 Orange Street, Suite 600, One Commerce Center, Delaware

19801. Hipster is not presently registered to conduct business in Texas and has not designated an agent for service of process in Texas. Hipster may be served and has been served in this action by certified mail, return receipt requested, directed to Hipster via its registered Delaware agent at its principal place of business through the Texas Secretary of State as its agent for service of process at Citations Division, 1019 Brazos, Austin, Texas 78701: via either 330 Townsend Street, Ste. 202, San Francisco, California 94107 or 3130 Lowell Ave., California 90032-2913.

33. ***Defendant Instagram, Inc.*** ("Instagram") is a Delaware corporation with its principal place of business at 181 South Park Avenue, San Francisco, California 94107. Instagram has appeared in this action.

34. ***Defendant Kik Interactive, Inc.*** ("Kik Interactive") is a Canadian corporation with its principal place of business at 420 Weber St. North, Unit I, Waterloo, N2L 4E7, Canada. Kik Interactive has appeared in this action.

35. ***Defendant Path, Inc.*** ("Path") is a Delaware corporation with its principal place of business at 400 2nd Street, Suite 350, San Francisco, California 94107. Path has appeared in this action.

36. ***Defendant Rovio Mobile Oy*** ("Rovio") is a Finland corporation with its principal place of business at Keilaranta 19 D 02150 Espoo Finland. Rovio has appeared in this action.

37. ***Defendant Twitter, Inc.*** ("Twitter") is a Delaware corporation with its principal place of business at 795 Folsom Street, Suite 600, San Francisco, California 94107. Twitter has appeared in this action.

38. ***Defendant Yelp! Inc.*** ("Yelp") is a Delaware corporation with its principal place of business at 706 Mission Street, San Francisco, California 94103-3162. Yelp has appeared in this action.

39. ***Defendant ZeptoLab UK Limited aka ZeptoLab*** ("ZeptoLab") is a United Kingdom limited company with its principal place of business at 11 Staple Inn Buildings, London, United Kingdom WC1V7QH. ZeptoLab has appeared in this action.

40. The plaintiffs and defendants are collectively referred to herein as the "Plaintiffs" and "Defendants," respectively.

41. The following Defendants are collectively referred to as the "App Defendants": Chillingo, Foodspotting, Foursquare Labs, Gowalla, Hipster, Instagram, Kik Interactive, Path, Rovio, Zepto Labs, Twitter, Yelp, and Facebook (for any period it controlled or operated Gowalla or its App)

JURISDICTION AND VENUE

42. This Court has subject matter jurisdiction over this action under:

(a) 28 U.S.C. § 1331 (federal question);

(b) 28 U.S.C. § 1332(d) (the Class Action Fairness Act) because (i) there are 100 or more Class Members, (ii) at least one Class Member is a citizen of a state that is diverse from any Defendant's citizenship, and (iii) the matter in controversy exceeds $5,000,000 USD exclusive of interest and costs;

(c) 18 U.S.C. § 1030(g), *et seq.* (civil actions under the Computer Fraud & Abuse Act);

(d) 18 U.S.C. § 1964 (civil actions under the Racketeer Influenced & Corrupt Organizations Act);

(e) 18 U.S.C. § 2201 (declaratory relief under the Declaratory Judgment Act); and,

(f) 18 U.S.C. § 2520, *et seq.* (civil liability under the Electronic Communications Privacy Act).

This Court also has subject matter jurisdiction over Plaintiffs' related state law claims under 28 U.S.C. § 1367.

43. This Court has personal jurisdiction over the Defendants. At all relevant times, each Defendant conducted substantial business in the Western District of Texas. Gowalla's principal place of business and registered office are in this judicial district. The remaining defendants have transacted business within this judicial district and had sufficient minimum contacts with Texas and this judicial district so that they are amenable to service of process under the Texas long-arm statute (TEX. CIV. PRAC. & REM. CODE §§ 17.041-.045) and FED. R. CIV. P. Rule 4(e) and so that requiring them to respond to this action would not violate due process.

44. Venue is proper in the Western District of Texas under 28 U.S.C. §§ 1391(b) and (c) because, as described herein:

(i)Most Plaintiffs and defendant Gowalla reside within this judicial district;

(ii) defendants Apple, Electronic Arts, Gowalla and Facebook have offices, personnel and operations within this judicial district;

(iii) each Defendant conducts substantial business in this judicial district, including placing their Apps on multitudes of Texans' iDevices, collecting and paying Texas sales taxes on App sales to Texas residents, taking without authorization the address books from Texans' iDevices, and the following business related to their Apps:

a. Rovio attended and participated in the 2011 South By Southwest Interactive festival ("SXSWi") in Austin, Texas and promoted and launched an *Angry Birds* App at SXSWi 2012;

b. ZeptoLab submitted a proposed panel entitled *Cut the Rope: Mobile to Global* to the 2012 SXSWi festival;

c. Foodspotting launched its App at the 2010 SXSWi festival and participated in and held several public promotions for its App and its business around Austin during the 2011 and 2012 SXSWi festivals;

d. Foursquare Labs launched its App at the 2009 SXSWi festival and has participated in and held numerous promotions around Austin during each of the SXSWi festivals since then;

e. Hipster held events and promotions in Austin during 2011 and 2012 SXSW festivals to recruit engineers and employees and promote its App;

f. Kik Interactive participated in the 2011 SXSWi festival and promoted and marketed its Kik Messenger App at the festival and around Austin;

g. Instagram participated in 2011 and 2012 SXSWi festivals and displayed, promoted and marketed its App at the festival and around Austin;

h. Path's CEO attended the 2012 SXSW festival and promoted Path's App;

i. Twitter has participated in every SXSWi festival since 2007, where it essentially launched with promotional video screens around the Austin convention center posting festival attendees' "tweets";

j. Yelp has personnel based in Austin, regularly contracts and works with Austin businesses, and promotes its service and its App around Austin during SXSW festivals;

(iv) a substantial part of the events or omissions giving rise to these claims occurred within this judicial district; and,

(v) a substantial part of the personal property that is the subject of this action—i.e., the iDevices and the owners' personal address books that were maintained on and taken from their iDevices—is situated within this judicial district;

(vi) violations of criminal law occurred or were initiated in Austin, Texas.

45. All causes of action are based on the same operative facts.

CLASS ACTION ALLEGATIONS

46. Plaintiffs bring this lawsuit as a class action under Rules 23(a), 23(b)(1), 23(b)(2) and/or 23(b)(3) of the Federal Rules of Civil Procedure on behalf of a Class of similarly situated persons consisting of:

> Plaintiffs and all owners of iDevices who obtained Apps from Apple's App Store that without requesting the iDevice owner's prior consent initiated an unauthorized iDevice call following which the owner's address book materials were copied, uploaded, transmitted, and/or disclosed to others and/or remotely stored and/or otherwise remotely used by others, including any of the following Apps: *Angry Birds Classic, Crystal, Cut the Rope, Foursquare, Foodspotting, Gowalla, Hipster, Kik Messenger, Instagram, Path, Twitter*, or *Yelp!* (the "Class") and who were damaged thereby.

Excluded from the Class are the Defendants and their officers, directors, managing agents and subsidiaries, members of Defendants' immediate families, the Court and any Court personnel, and the legal representatives, heirs, successors or assigns of any excluded person or entity.

47. Numerosity: The Class is so numerous that joinder of all members is impracticable. The precise number of Class members can only be ascertained through discovery from the Defendants. However, widespread consumer adoption of iDevices and the reported multi-million-person installation bases for the offending Apps listed in this Complaint indicate that the putative Class consists of in excess of five million persons, making joinder impracticable. Disposition of this matter as a class action will provide substantial benefits and efficiencies to the parties and the Court.

48. Typicality: The named Plaintiffs' claims are typical of the claims of the Class members as all members are similarly affected by the Defendants' wrongful conduct in violation of the federal and state laws described herein. Indeed, the rights of each Class member were violated in a virtually identical manner—i.e., without consent each Class member's iDevice made an unauthorized call, accessed, copied and uploaded each Class member's private address book, and disclosed and transferred the address book to others who remotely stored and/or used it in violation of federal and state laws—as a result of the Defendants' actions and/or inactions. More specifically, Apple marketed, distributed, downloaded to and installed on consumers' iDevices numerous malicious Apps (including those listed herein), which were supposedly validated and pre-approved by Apple, that each similarly transferred the Plaintiffs' and the Class members' private address books from their iDevices and disclosed them to others who used them, all without requesting permission or receiving consent to do so.

49. Commonality: Common questions of law and fact exist as to all members of the Class and predominate over any questions solely affecting individual members of the Class. Among the issues of law and fact common to the Class are:

- iDevice owners' reasonable expectation of privacy and ownership and proprietary interests in their iDevices and their private address books;
- promises and representations made by Apple and other Defendants to iDevice owners and consumers, including those related to the privacy and the security of their address books and iDevices;
- whether the Defendants' Apps constitute malware or spyware;
- can Apple abrogate all consumer protections and other laws for itself and the App Defendants when they make, sell and distribute harmful Apps;
- did the Defendants wrongfully obtain, use, store or keep iDevice owners' address books or derivatives thereof;
- did the Defendants cause consumers' iDevices to, without requesting the owner's consent or in ways exceeding any purported consent, initiate calls and access, copy, transmit, upload and disclose bulk portions of the Class members' private address books, and then remotely store and/or use those address books;
- the commercial market value of the Class members' address books and of contact data points and data fields typical of those contained in the Class members' iDevice address books and the technical methods used by and benefits realized by any Defendants who improperly gleaned such address book materials from the Class members' iDevices;
- what standards of care must be afforded to consumers, iDevice owners and private address books maintained on consumers' iDevices and what levels of protection are mandated under Apple's application developer policies and agreements;
- what laws did Defendants violate and what injunctive equitable or declaratory relief or statutory, actual and other damages arise and are awardable if Defendants committed the acts alleged herein;
- whether consumers and the Class members are beneficiaries of the agreements between App Defendants and Apple or of Apple's developer guidelines and standards;

- how to interpret any disclosures, guidelines, policies, agreements, alerts or pop-up dialogue boxes that may be resident in or appended to Defendants' various Apps and iDevices and the validity, enforceability, unconscionability, and/or adhesive nature thereof and interactions between the same;

- whether the acts alleged herein violate the state and federal laws prohibiting fraud and related activity in connection with computers, interception, disclosure or use of wire or electronic communications, theft or transportation of stolen property, breach of computer security, related racketeering activities, and common law misappropriation, conversion, invasion of privacy or unjust enrichment;

- an App distributor's (and iDevice manufacturer's) direct, independent and/or joint and several responsibility and liability for products, services, and software promoted on, offered over, approved by and distributed via its sales platform and (supposedly) tested and pre-cleared by that provider under policies and procedures that should have prevented non-compliant, Trojan-horse-like malicious apps—here, ones that make unauthorized calls and expose and facilitate the taking and use of the iDevice owner's private address books—from reaching the market or being available to the Class members;

- did Defendants act knowingly, intentionally, maliciously, wantonly or recklessly in connection with their conduct alleged herein; and,

- whether the members of the Class have sustained compensable or statutory damages and, if so, the proper measure of damages.

50. Plaintiffs and their counsel will fairly and adequately represent the interests of the Class. Plaintiffs have no interests contrary to or in conflict with those of the Class members. Plaintiffs' retained counsel have competently identified recoverable Class claims and are sufficiently competent and experienced with the prosecution of cases before this Court and in this judicial district, including complex small and large scale disputes involving technology, privacy and civil rights, misappropriation of data and information, and electronic piracy and RICO violations and have worked and served as counsel on both federal and state class action matters. Plaintiffs' counsel have obtained benefits for the Class already, as evidenced by (a) defendant Apple's announced in-progress modification of its iDevices and iOS to purportedly inhibit non-consensual access to or transmission of iDevice owners' address books; and (b)

defendant Path's announcement after the filing of this lawsuit that its App would anonymize all uploaded user address book materials and request explicit user approval before such uploads.

51. Plaintiffs know of no difficulties to be encountered in the management of this action that would preclude its maintenance as a class action, either with or without sub-classes.

52. A class action is superior to other available methods for fairly and efficiently adjudicating this controversy, especially since joinder of all Class members is impracticable. Plaintiffs and the Class members have been irreparably harmed as a result of the Defendants' wrongful conduct. Litigating this case as a class action will reduce the risk of repetitious litigation relating to the Defendants' conduct.

53. As the damages suffered by individual Class members may be proportionately small, the expense and burden of individual litigations make it virtually impossible for Class members to individually redress the unlawful conduct alleged and wrongs done to them on a cost-effective basis. That burden would substantially impair the ability of Class members to pursue individual lawsuits to vindicate their rights. Consequently, absent a class action, Defendants would retain the benefits of their wrongdoing despite the serious nature of their violations of the law.

54. Accordingly, class certification is appropriate under Rule 23.

55. The allegations herein apply equally to all Class members, who each have been identically subjected to Defendants' described wrongdoings and suffered identical harms to Plaintiffs.

BACKGROUND
APPLE AND THE APP DEFENDANTS' CONDUCT

56. According to news reports and company admissions, Plaintiffs' Apple-manufactured "iDevices" have, on their own and without Plaintiffs' consent, initiated calls and

surreptitiously uploaded, transmitted and disclosed Plaintiffs' valuable private address books to others. According to Apple, Plaintiffs' iDevices were not supposed to do that.

57. These unauthorized uploads and takings of Plaintiffs' private address books, which occurred numerous times via Wi-Fi, cellular networks and the Internet, began to occur after Plaintiffs added Defendants' Apps to their iDevices from Apple's App Store and used those Apps. According to Apple, Apps obtained from the App Store would not violate iDevice owners' rights of privacy, surreptitiously attempt to discover private user data, transmit materials from the iDevice without notice to and authorization from the iDevice owner, or contain malware. But these did.

58. Although Apple publicly claims it tested and "rigorous[ly] review[ed]" all Apps (and their associated documentation), including each of Defendant's Apps, for compliance with mandated standards—including protecting iDevice owners' privacy and preventing unauthorized transmissions—before approving, digitally-signing and voluntarily releasing and distributing them on its App Store, it nonetheless distributed these malicious Apps to Plaintiffs. In so doing, Apple fell far short of its specified and industry-standard levels of care and violated its promises to consumers.

59. As a result, the App Defendants were able to effectively steal Plaintiffs' address books from their iDevices. Until it was publicly reported in February 2012, Plaintiffs did not know that the App Defendants had secretly obtained their address books and forwarded them to others' servers where they were stored and used.

60. Rather, Defendants each promised to protect iDevice owners' privacy and private information and to acquire and use only those materials consensually transmitted from owners' iDevices. The App Defendants also represented and promised that their Apps would comply with

Apple-mandated standards as well as all laws in any location where the App is made available to users. Of equal significance, all Defendants represented and promised that their Apps would not surreptitiously attempt to obtain private user data or, or contain malware. But they did.

61. Following a NEW YORK TIMES exposé in February 2012, officials at Defendants Foodspotting, Foursquare Labs, Hipster, Path, and Twitter confirmed that their Apps were triggering unalerted iDevice address book transmissions from all or a portion of their respective iDevice App user base and that their companies had been receiving, remotely using and storing iDevice owners' address books.

62. Path and Hipster's CEOs, Dave Morin and Doug Ludlow, issued written public apologies and admitted that they "made a mistake" and "clearly dropped the ball when it comes to protecting our users' privacy."

63. Apple agreed, concurrently announcing that:

> "Apps that collect or transmit a user's contact data without their prior permission are in violation of [Apple's] guidelines . . .."

64. Additionally, technical experts posted numerous analyses and reports identifying Apps from the remaining Defendants as ones that were also secretly uploading and transmitting iDevice owners' address books without permission.

65. While these Apps were facilitating the taking of address books from consumers' iDevices, Plaintiffs had the App Defendants' Apps, and had taken the steps necessary for the thefts to silently occur. More particularly, Plaintiffs to the extent necessary, registered on the App, navigated to screens, and/or tapped button displays in the App Defendants' Apps that triggered the theft. As a result, Plaintiffs each had their private iDevice address book materials copied, transmitted, uploaded**,** stored, used and disclosed without their consent.

66. On information and belief, the App Defendants received via the Internet, remotely used, and stored bulk portions of Plaintiffs' private address books taken from their iDevices.

67. Neither Apple nor the App Defendants warned Plaintiffs or alerted them in the Apps or on their iDevices that their private address books were being taken from their iDevices and transmitted and disclosed to others.

68. More particularly, Defendants never asked Plaintiffs to consent to, agree to, or pre-authorize the unalerted, surreptitious transmission or disclosure of their private address books from their iDevices to others.

69. Nor was Apple disinterested on the sidelines. Apple acted as the App Store gatekeeper and self-proclaimed protector of consumer privacy. In fact, in 2008, Apple removed the *Aurora Feint* App for transmitting iDevice owners' private address books without first asking and getting owners' approval.

70. Thus, Apple adhered to – or at least appeared to adhere to and enforce for a time – its guidelines.

71. Despite knowing that it had left its iDevices owners' address books exposed and insecure, and that its review process was flawed, Apple permitted the App Defendants' distribution of malicious Apps to Plaintiffs' and other consumers' iDevices.

72. Apple also never notified the Plaintiffs or its iDevice owners after the fact that Apps on their iDevices had been surreptitiously taking their private address books. Apple never recalled any of these Apps or provided refunds on any of these Apps. Nor did Apple remove these Apps from the App Store or terminate them from its App developer program, as supposedly required.

73. Conversely, in mid-2012 Apple removed *Clueful*, an App from a noted technology security company, BitDefender, whose App warned iDevice owners of other App Store apps that silently took materials from their iDevices.

74. In late 2011, Apple also banned security researcher Charlie Miller for a year for reporting to Apple a security hole in its App procedures after he passed a non-compliant app through Apple's "review" and onto its App Store.

75. As the App Defendants' Apps meet Apple's published definitions for malware, the App Defendants' combined with Apple to distribute harmful malware via the App Store to Plaintiffs' and consumers' iDevices. Both Apple and the App Defendants promised not to put this on Plaintiffs' iDevices.

76. Thus, Plaintiffs have been harmed and damaged by Defendants' acts.

77. For example, Plaintiffs' private address books have intrinsic, extrinsic and commercial market value. Companies, like Lead411, purchase address books from ordinary consumers and even solicit such purchases via the Internet. Also, industry reports value individual address book contacts at roughly $0.60 to $3.00 apiece. Thus, Plaintiffs, who all have had more than one hundred contacts on their iDevices at all relevant times, lost at least this much per contact.

78. Plaintiffs' private address books also contain incredibly personal and private information. Thus, Defendants de-privatized Plaintiffs' private address books and eliminated Plaintiffs' ability to control and keep the information private.

79. In fact, the App Defendants unilaterally transformed Plaintiffs' private address books from materials considered private and subject to Constitutional protections – including Due Process prohibitions against warrantless seizures and First Amendment protections from

disclosure under privacy and freedom of association principals – into non-private, public materials that may now be obtained from Defendants and inquired into by government officials without a warrant or cause or that may be sold by Defendants. As a result of Defendants' acts, Plaintiffs' private address books have been commercially devalued and de-privatized and the App Defendants have impermissibly benefited by growing their social and gaming networks exponentially, and by Apple gaining customers.

80. Moreover, the surreptitious address book uploads and transmissions were reportedly often unencrypted and made over open wireless access points in coffee shops, restaurants, stores and businesses, turning the Plaintiffs' iDevices into Wi-Fi mobile beacons broadcasting and further exposing the unsuspecting Plaintiffs' address books to the public.

81. These unauthorized transmissions used iDevice resources, battery life energy and cellular time, at a cost to the Plaintiffs, and caused loss of use and enjoyment of some portion of their iDevices' useful life. As Plaintiffs must also re-charge their iDevices, the Defendants' actions have resulted in the consumption of additional electricity purchased by Plaintiffs.

82. Plaintiffs are also entitled to have their iDevices repaired or modified to prevent similar surreptititious address book intrusions in the future and their hardware and date integrity validated by an expert technician and repaired as needed.

83. Plaintiffs purchased iDevices – at a cost of several hundred dollars a piece – that were commercially represented to be personal devices that emphasized security and privacy. As it turns out, the iDevices Plaintiffs purchased lacked the privacy features, at least with respect to the address book, Apple had touted. Accordingly, they are less valuable and useful than they were represented to be and Plaintiffs effectively overpaid for those iDevices and suffered various harms.

iDEVICES - GENERALLY

84. The iPhone is a mobile smartphone. The iPad is a tablet computer. The iPod touch is a digital music player. Each of these consumer products were designed, made and marketed by Apple.

85. They feature a computer processor, a multi-touch interface (i.e., a touch screen visual display), built-in Wi-Fi, wireless networking, and the ability to wirelessly receive and use "Apps" that provide iDevice feature enhancements.

86. Apps appear as icons on an iDevice's touch-screen visual display and activate and operate when the iDevice user touches displayed on-screen icons and buttons.

87. iDevices come with a written warranty and with an iPhone or iOS software license ("iOS SLA"), which purportedly licenses the consumer to use the software that comes with and is on the iDevice.

88. Apple has repeatedly told consumers, including Plaintiffs, in writing and at conferences that "Apple respects your privacy" and that it does not allow Apps to take private information without asking. Apple had never corrected these statements.

THE iDEVICE BUILT-IN "CONTACTS" APP

89. Each iDevice comes with several integrated built-in Apps that enable a variety of functions. One built-in App that Apple designed and supplies with all iDevices is entitled "Contacts." The "Contacts" App is designed and functions to maintain the iDevice owner's personal address book. On information and belief, the "Contacts" App is part of each iDevice's iOS operating system.

90. Plaintiffs used their iDevice "Contacts" App, as encouraged by Apple, to organize and maintain their address book contacts. Plaintiffs each inputted numerous address book

contacts on their iDevices at relevant times prior to February 6, 2012. Each Plaintiff had more than one hundred contacts in their address book.

91. iDevices and the "Contacts" App, by design, take in from other sources the iDevice owner's existing address book materials via wire, wirelessly and over the Internet. When connected to a designated computer or network, the iDevice syncs itself by communicating electronically with and transferring to the iDevice the owner's private address book and other materials from the computer or network.

92. Plaintiffs each synched their iDevices numerous times during the relevant time in which Defendants were taking iDevice owners' address book materials.

THE iDEVICE'S "APP STORE" APP AND APPLE'S APP STORE FOR ADDITIONAL APPS

93. Another built-in App on all iDevices is entitled the "App Store." The "App Store" App allows an iDevice owner to browse for and obtain additional Apps available from Apple and to update Apps already on the iDevice.

94. Apple also owns and operates an off-device App Store, a centralized repository of Apps available for iDevices combined with a digital App distribution platform for marketing and wirelessly delivering iDevice-compatible Apps to every iDevice user.

95. Apple makes Apps for iDevices available to consumers, including Plaintiffs, exclusively through its App Store, and takes 30 percent of the revenues charged on each App downloaded and delivered by the App Store.

96. On information and belief, Apple stores and indexes the available Apps on its own servers, or servers that it manages and controls, before delivering selected Apps to consumers.

97. Customers receive no physical product when they obtain an App from the App Store. Apps are delivered wirelessly to their iDevice and automatically deployed on the iDevice by the on-device "App Store" App.

98. To oversee App content and functionality, Apple created, operates and manages an App iOS Developer Program, which it uses to guide and cull Apps created and intended for release to iDevice users via the App Store. Apple charges a $99 annual fee to participate in the program. Apple now receives almost $50 million in annual revenues from these fees. Upon information and belief, the App Defendants each paid this fee and participated in the program. Apple chooses which Apps to make available on the App Store and, according to Apple, vets each App before it is issued or updated.

99. Apple marketed these pre-vetted Apps on its App Store since July 10, 2008 and decides how and which Apps to feature. Apple now markets and distributes over 500,000 Apps to roughly 315 million iDevice consumers, such as Plaintiffs, over the App Store.

100. The availability of an increasing number and selection of Apps and the expandable iDevice functionality drives sales of iDevices.

101. Apple's marketing and advertising touts its App Store and the availability of Apple-approved Apps as an important reason for consumers to purchase iDevices and Apple expends significant resources advertising their availability.

102. Apple forces consumers to go through its App Store to obtain Apps for their iDevices. In fact, as manufactured, iDevices work only with Apps obtained from Apple's App Store that have been approved by Apple and for which Apple has provided a digital certificate.

103. After Apple approves and provides a digital certificate for the App, Apple then markets, distributes and sells the App through the App Store - collecting all gross revenues and

sales taxes. Apple retains 30% of the sales price of an App or any subsequent "digital goods" sold through an App and 60% of any additional future revenues from Apps that incorporate Apple's iAd advertising program, which first launched in 2010. Apple pays any applicable state sales tax based upon the account address it has of the recipient iDevice owner.

104. Consequently, Apple has monetary and business incentives to offer a wide selection of and distribute as many Apps as possible—it makes money on and through them, even if they are "free".

APPLE'S APP DEVELOPER PROGRAM AND APPLE'S CONTROL OVER THE SELECTION, APPROVAL AND RELEASE OF APPS ON THE APP STORE

105. Just as Apple forces consumers to go through Apple to obtain Apps, Apple similarly forces App creators to go exclusively through Apple, its App Developer Program, its testing, review and legal clearance process, its selection committee, its transaction processing system, and its App Store to get Apps to consumers' iDevices. On information and belief, the App Defendants did so.

106. Apple is the exclusive purchase, distribution and sales point for valid Apps and manages all administrative matters associated with App transactions. Apple establishes and maintains the right to enforce legal and technical standards and policies and guidelines that Apps must meet, and purports to review and test submitted Apps pre-release for compliance with those standards. Apple unilaterally decides which ones will be offered to iDevice owners.

107. Apple voluntarily chose to structure its iDevice App review and selection process this way. By comparison, Google-backed Android devices offer an open environment more similar to an ordinary retail marketplace. Android device owners may obtain Android-compatible Apps from whatever source makes them available, including directly from the creator of any particular App. On information and belief, Apple selected its "walled garden" model so that it

could exert full control over the content, selection, availability, and security of Apps for consumers' iDevices.

108. On information and belief, the App Defendants each followed Apple's standard protocol for getting Apps on the App store.

109. Anyone wishing to submit an App to the App Store must first participate in Apple's iOS Developer Program by paying Apple a $99 yearly registration fee and executing Apple's standard-form iPhone Developer Program License Agreement ("IDPLA").

110. The IDPLA serves, in part, as a license agreement, authorizing program participants to use proprietary Apple software and code to build iDevice Apps. Together, the Apple software (collectively known as the Apple iOS "Software Development Kit" or "SDK") and registered App developer program provides program participants access to a wealth of information, tools, diagnostics and technical support services that Apple designed and published to facilitate the development of Apps for Apple's iDevice products.

111. The resources Apple provides to program participants include editing software, simulators, forums, guides, design and approval criteria, code, code resources and libraries, performance enhancing tools, testing software, and mentoring via access to Apple engineers who "provide … code-level assistance, helpful guidance, [and] point [the developer] towards the appropriate technical documentation to fast-track [his/her] development process."

112. Despite Apple's statements to the public that Apple protects consumer privacy, Apple's tutorials and developer sites specifically teach App developers how to code and create Apps that non-consensually access, manipulate, alter, use and upload the address book maintained on an owner's iDevice.

113. On information and belief, the App Defendants were each aware of this and their personnel utilized these tutorials and developer sites.

114. To get applications into the App Store, Apple requires program participants to submit their Apps for approval or rejection by Apple. Apple purports to review every app on the App Store based on a set of technical, content, and design criteria, as well as for reliability, offensive material, malware and privacy issues. Thus, Apple purports to protect iDevice owners against the type of harmful Apps Plaintiffs instead received. On information and belief, Apple did review and approved each of the App Defendants' Apps despite their malicious nature.

115. Apple also requires each App developer to re-submit his or her App for testing and compliance verification whenever a change, update or new version is created, and retains the authority to terminate sales or distribution of any App and/or terminate the account of any App developer for non-compliance with Apple's development policies and standards.

116. On information and belief, Apple reviewed all updates and new versions of the App Defendants' Apps, and did not terminate or restrict their distribution at any time even thought they were secretly uploading Plaintiffs' addres book materials.

APPLE HAS ESTABLISHED ITS APPS ARE SUBJECT TO VARIOUS STANDARDS OF CARE

117. Based on their agreements and actions, Apple and the other Defendants have a duty to not publicly release to consumers and iDevice owners iDevices, iOS versions and Apps that do not meet standards of care established by Apple, by the industry and by law. These include not creating malware and not taking consumers' private information without permission.

Apple-established standards

118. Via its iOS Developer Program and agreements, IDPLA, SDK, published App Store Review Guidelines, other published guidelines and policies, and public statements, both

generally and to the FCC, Apple sets standards of care for itself and others regarding Apps available on and distributed from the App Store. For example, informed the FCC that its Apps "must not contain malware or harmful code" and Apple's App Store Review Guidelines specifically state that:

- Private data – like address books – may not be obtained without the users' consent;
- apps may not have secretly hidden features;
- and Apps must comply with local legal requirements in all states to which they are distributed, even state tort law.

119. Apple is also crystal clear and informed the App Defendants that malware – which is prohibited – includes software that can violate your privacy.

120. According to then Apple CEO, Steve Jobs, a malicious application is one like Foursquare, Path, and the other App Defendants' Apps that take users' personal information without permission.

Industry Standards

121. Nor is Apple the only platform that sets standards, limits the Apps that will be sold or distributed over their marketplaces and promotes App protection of private user address books and other data. Google and Amazon.com do as well.

122. Google and Amazon.com also have digital distribution platforms for the sale and distribution of Android-compatible Apps. Both limit the Apps that will be sold or distributed over their marketplaces, require Apps to comply with privacy standards, and prohibit the taking of private information, such as address books, without the user's consent. Amazon.com prohibits even Apps that only "have the potential to infringe upon an individual's privacy."

123. Accordingly, the three main industry participants each have set similar minimum App standards, including: (1) Apps must comply with all applicable laws; (2) Apps must protect

user privacy and private information; (3) Apps must notify users in advance and obtain permission from App users prior to accessing or obtaining personal or private information from the user's device. These standards apply to all App developers and Apps released to the public.

APPLE REPRESENTATIONS ON iDEVICES, APPS AND APP STORE

124. Apple has made numerous public representations and assurances to consumers and these Plaintiffs regarding its iDevices, App Store and Apps distributed from its App Store.

125. Apple acknowledged its standards of care as listed in the preceding section apply to Apps released to the public over the App Store under its iOS Developer Program.

126. Apple, as an App developer itself, must comply with the same standards mandated upon others distributing Apps via the App Store.

127. Apple publicly states that consumers should feel comfortable and safe obtaining pre-approved Apps from Apple's App Store. Apple assures consumers such as Plaintiffs that Apps from Apple's "curated App Store" are"rigorous[ly] review[ed]," tested for compliance with numerous guidelines, and do not "suck up consumers' private information." During a September 2008 public presentation, Apple CEO Steve Jobs similarly stated, albeit falsely in retrospect, that the App Store was not going to distribute malicious apps or apps "that invade your privacy" and that the App Store supposedly provided Plaintiffs and consumers, "freedom from programs that steal your private data [and] freedom from programs that trash your battery."

128. Apple explicitly assured Plaintiffs that: "Apple respects your privacy" with every App transaction.

129. Thus, Apple represents (and instructs developers) that "***the Address Book database is ultimately owned by the user***" that "privacy is vitally important," that Apps that collect or transmit a user's contact data without their prior permission violate its guidelines, and

that Apps that suck your personal data to the cloud will be rejected. Apple even stated, "Applications on the device are 'sandboxed' so they cannot access data stored by other applications."

130. In fact, Apple told FCC in a 2009 letter that it keeps publically posted on its website not only that malware is not permitted on the App Store but that protecting consumer privacy is at the core of its App review process.

131. Neither Mr. Jobs nor Apple has ever disavowed to consumers, iDevice users, or Plaintiffs any of these statements, representations or promises.

132. Thus, with its contract with App developers and all its public interactions, Apple represents that it protects consumers' privacy directly and that it expects App developers to do so as well. In fact, from 2008 to the present, the highest levels of Apple from its founder to its current CEO to its corporate spokesman have so consistently expressed that Apple protects its customers' privacy that – although inaccurate – it is ingrained in the image of Apple's culture and marketing as well as in the minds of customers. Apple has never corrected this falsity.

APPLE ENCOURAGES DATA THEFT

133. Apple also contractually requires iOS Developer Program participants to abide by its *iOS Human Interface Guidelines* developer reference manual included in Apple's iOS DEVELOPER LIBRARY, which states:

- at p. 47: "Get information from iOS, when appropriate. People store lots of information on their devices. When it makes sense***, don't force people to give you information you can easily find for yourself, such as their contacts*** or calendar information."

- at p 48: "***iOS devices are personal devices***, but they also encourage collaboration and sharing with others. Enhance your app by helping people collaborate and connect with others.
  When appropriate, ***make it easy for people to interact with others and share things*** like their location, opinions, and high score . . .. ***People generally expect to be able to share***

information that's important to them."

- at p. 63: "It's often said that ***people spend no more than a minute or two evaluating a new app. . . . Avoid displaying an About window or a splash screen***. In general, try to ***avoid providing any type of startup experience that prevents people from using your application immediately. Delay a login requirement for long as possible***. Ideally, users should be able to navigate through much of your app and understand what they can do with it before logging in."

- at p.65: "If possible, ***avoid requiring users to indicate their agreement to your EULA when they first start your application.*** Without an agreement displayed, users can enjoy your application without delay."

134. Thus, quite the opposite of the standards it espouses and purportedly mandates, Apple teaches and suggests in its *iOS Human Interface Guidelines* that program participants design Apps to: (a) directly and automatically access contact data—particularly whenever it is desired by a developer for collaborative or sharing purposes—without any prior alert(s) to the user; and (b) be downloaded, operate, and function in advance of any presentation of or user consent to any End User License Agreement ("EULA") and/or privacy policy (assuming that ones even exists). Indeed, the App Defendants never presented any EULA, terms of service, privacy policies or other agreements to Plaintiffs in advance of their respective Apps being downloaded to and first operating on Plaintiffs' iDevices, to the best of Plaintiffs' recollection.

135. Consequently, despite supposedly mandating that program participants' Apps not include surreptitious data harvesting functionalities (and supposedly reviewing and testing all Apps to ensure the absence of forbidden functionalities), Apple taught App developers to incorporate forbidden surreptitious data harvesting functionalities—even for private "contacts"—into their Apps and encouraged program participants to design those functions to operate in non-obvious manners. On information and belief, the App Defendants did just that.

UNDISCLOSED MATERIAL INFORMATION

136. Apple never disclosed to consumers, iDevice users, or Plaintiffs, either in connection with the iDevice, the iOS, the Apple-supplied "Contacts" App or "App Store" App, the App Store or any other App, that their iDevices, iOS or Apps would or could, either alone or in combination with an iDevice self-transmit the iDevice owner's address book without the authorization of the iDevice owner. Apple has known of this risk and that App developers and Apps—such as the *Aurora Feint* then *Gowalla,* then *Kik Messenger*—have been again and again exploiting this security hole and surreptitiously taking address book materials since as early as 2008. To this day, Apple still has not warned or notified iDevice owners of that risk.

137. Prior to February 2012, none of the Defendants (with the exception of Kik Interactive) publicly disclosed that inclusion of their Apps on iDevices would or could, in combination with an iDevice and/or iOS, cause the iDevice to self-transmit the iDevice owner's address book without the authorization of the iDevice owner. And Kik Interactive did not disclose that its App was doing so, either, until it was caught red-handed and media reports appeared discussing its hyper-kinetic user-base growth.

THE APP DEVELOPERS

Aurora Feint – Strike One

138. In July 2008, Apple delisted the popular *Aurora Feint* game App from the App Store for a few days after it was revealed to be *uploading iDevice users' contact lists* to the game maker's servers without first asking users if it could do so.

139. Somehow, the App made it past Apple's "comprehensive" and "rigorous" testing and review process and, when released on the App Store, soared to the top of the popularity list via its automated address-book-harvesting and networking-fueled growth.

140. After just three days off the App Store, it returned—missing the malicious code portion of its delisted release—with Apple's approval and promotion of the App to the *What We're Playing* App Store list.

141. Apple thus was almost immediately aware that App developers were inclined to exploit the security hole surrounding the ease of access to iDevice address book contacts and do what they wished with owners' private mamterials.

iAd

142. In July 2010, Apple launched its iAd mobile advertising platform, which allowed Apps to display targeted in-App ads and instantly made Apple and its App developers advertising partners; they split the ad revenues 60/40.

143. Previously ad-free iDevices were also automatically opted-in to the iAd program by Apple and, through the iDevices, Apple gathered detailed demographic information on its millions of users and delivered them highly-targeted ads.

144. Consequently, iDevice owners were no longer just Apple's customers; they were now also Apple's *product*.

145. Following this development through the filing of this action, apparently no app developer's App was again removed from the App Store for reported address book privacy issues, as *Aurora Feint* had been earlier, even though malicious non-compliant apps were regularly being issued with Apple's approval.

***Gowalla* – Strike 2**

146. For example, a team of professors and doctoral graduate student computer scientists investigated "privacy leaks" of private data and sensitive information from iDevices in 2010 and noticed that the *Gowalla* App was, without prior permission, uploading and

transmitting the iDevice's address book—names and email addresses particularly—in its entirety to the developer when the user viewed contacts through the App.

147. Defendant Gowalla authored the *Gowalla* App, with Apple providing assistance through the iOS Developer Program and a digital certificate for the App to function on iDevices. Following Apple's review, Apple released and distributed the *Gowalla* App on the App Store.

148. The scientists in 2010 provided Apple a "detailed report" of what the *Gowalla* App was doing through Apple-designated channels for problem reporting, even providing screen shots of the unencrypted transmission of the address book, and later reported this in a peer-reviewed paper.

149. Apple, ignored them, stating, "If you have a privacy concern, you should contact the developer." With that, Apple apparently washed its hands of the matter.

150. Indeed, the *Gowalla* App remained available to iDevice owners on the App Store more than a year, until its successor, Facebook, eventually shut it down around December 15, 2011.

151. Here, the identified Plaintiffs each recall using the *Gowalla* App. More particularly, they recall logging in and navigating within the App to a "Find Friends" menu screen and being offered various options (including an option entitled "Address Book").

152. Plaintiffs do not recall being presented at any time with an intervening alert or display indicating that the Gowalla App would upload his or her address book to Gowalla or warning that such a transmission was about to occur.

153. On information and belief, by that point and ***before*** the user made any menu selection on the "Find Friends" page, the Gowalla App had ***already*** copied and uploaded iDevice

owners' address books, including Plaintiffs, without first asking or securing consent, to Gowalla's servers.

154. Before December 15, 2011, while each of the Gowalla Plaintiffs had the App when an iDevice *Gowalla* App user navigated to that screen, the iDevice would initiate a call, copy bulk portions of the user's address book, and the iDevice would then upload and transmit those materials via Wi-Fi, 3G and the Internet to Gowalla's servers, where Gowalla then remotely stored, used and kept the materials. This happened to Plaintiffs multiple times.

155. The *Gowalla* App never requested permission to upload any address book materials from Plaintiffs' iDevices or transmit any address book material off of Plaintiffs' iDevices.

156. Accordingly, Gowalla wrongfully obtained, retained, disclosed and de-privatized these Plaintiffs' valuable private address books and used their iDevices without authorization. Gowalla and its App never asked Plaintiffs if they could do any of these things.

***Kik Messenger* – Strike 3**

157. Gowalla was not alone. The *Kik Messenger* App was up to the same thing.

158. Defendant Kik Interactive authored the *Kik Messenger* App, with Apple providing assistance through the iOS Developer Program and a digital certificate for the App to function on iDevices. Following Apple's review, Apple released and distributed the *Kik Messenger* App on the App Store in late 2010.

159. Three weeks later, it had over two million users.

160. According to Kik personnel, the "secret sauce" behind *Kik Messenger's* eye-popping growth was that the App uploaded every email address contained in each new user's wireless mobile device's address book followed by an immediate "push" notification to both the

user and any matching email contact found in Kik Interactive's database. According to Kik, this all occurred automatically and without warning upon installation of the *Kik Messenger* App. Basically, Kik took and spammed the user's address book. On information and belief, this happened to Plaintiffs when they first used *Kik Messenger*.

161. Apple also knew of this because reporters wrote up numerous reports with titles like, "*Speedy Messenging App Kik Goes Viral, But is It Cool With Apple's T[erms]O[f]S[ervice]?*" and contacted Apple for an answer to that question. Apple chose again not to comment or warn consumers.

162. Accordingly, Kik Interactive wrongfully obtained, retained, disclosed and de-privatized these Plaintiffs' valuable private address books and used their iDevices without authorization. Kik Interactive and its App never asked Plaintiffs if they could do any of these things.

The Other App Defendants

163. As it turns out, numerous other App developers continued to exploit the address book security holes in the App Store's review and approval process and in the iDevices' "Contacts" App.

164. These surreptitious, unobservable iDevice address book thefts via App and Apple's bumbled secretive review and selection process were inherently undiscoverable and were not discovered until sometime after February 15, 2012. Accordingly, Plaintiffs assert, as necessary, the discovery rule and the doctrines of equitable tolling and fraudulent concealment on their claims herein.

165. In fact, disclosures came not from Apple, but the NEW YORK TIMES, which pointed out that App Defendants were surreptitiously taking address book data, including Defendants Hipster, Path, Twitter, Foursquare, Instagram, Yelp, Gowalla, and Instagram.

Path

166. Path is an photography App that allows iDevice owners to use their iDevices as a "personal journal" of one's life and its "moments" that could be "share[d] in a trusted, intimate environment."

167. Defendant Path authored the Path App with Apple providing assistance through the iOS Developer Program and a digital certificate for the Path App to function on iDevices. Following Apple's review, Apple released, distributed and marketed the Path App on the App Store.

168. Apple is also a joint-venture in the iFund venture capital fund and mentoring program ("iFund") with the venture capital company Kleiner Perkins. On information and belief, Path is an iFund company. On information and belief, Apple owns a portion of the iFund and provides mentoring to iFund-financed companies, including defendant Path and the iFund owns or owned a portion of Path's equity. On information and belief, Apple provided direct guidance, assistance and mentoring concerning the Path App.

169. In any event, Path consistently marketed itself to the App consumer marketplace and the public as a company focused on protecting App users' privacy.

170. On a company websites touting its App, Path stated that, "Path upholds the *expectations for privacy* of both the mobile phone and the journal with its limited, intimate, more personal network."

171. Similarly, Path founder and CEO Dave Morin stated in 2010 to a technology reporter that, "Path does not retain or store any of [the user's] information in any way."

172. Path also represented that its App is "private by default" and that its users "should always be in control of [their] information and experience.'" Morin publicly reiterated in 2011 that the Path App is "private by default and always will be."

173. These representations and statements were false and were never corrected by Mr. Morin or Path before February 6, 2012.

174. In fact, prior to this date, Path began taking, using and storing iDevice owners' address books without permission, including Plaintiffs, each of whom had downloaded the App prior to this time.

175. After Apple downloaded the Path App to the Plaintiffs' iDevices, each Plaintiff recalls opening the Path App, signing up via a "Sign Up" screen, and using and navigating around the Path App.

176. Before obtaining the Path App from the App Store or using it, the Path Plaintiffs were never told that Path's App would cause their iDevices to, without notification or permission, transmit and upload their private address books, or that Path would remotely store and use them. But that is what happened.

177. In early February 2012, programmer Arun Thampi reported on his blog that once an iDevice user signed up on Path's App, the App automatically and surreptitiously accessed and copied the iDevice owners' address book and initiated unauthorized iDevice transmissions that uploaded almost the entirety of the iDevice address book to Path's servers, where Path used, stored and kept those materials.

178. Myriad news reports and blogs picked up Mr. Thampi's blog and re-verified and re-reported his findings.

179. According to these reports, once the Path App was downloaded to an iDevice and the user registered for an account, the Path App automatically—without any additional notification to or input from the user—accessed and copied the iDevice's address book, made the Internet call "*https://api.path.com/3/contacts/add"* from the iDevice, and then wirelessly uploaded and transmitted to Path's company servers in a ".plist" the complete set of names, phone numbers, email addresses and even physical addresses maintained in the user's iDevice's address book.

180. On information and belief, the prior paragraph accurately describes how the Path App functioned following a user completing registration. On information and belief, this function occurred not only on registration, but also periodically upon re-launch of the App and following app updates.

181. Consequently, Path stole its users' address books, including the Plaintiffs', from their iDevices. These takings occurred before they even had a chance to use the Path App.

182. On February 8, 2012, Morin and Path apologized and acknowledged that Path had surreptitiously taken, used and stored address book materials from its users' iDevices prior to February 6, 2012, including Plaintiffs. Moreover, in an attempt to escape liability, Path deleted the evidence of its wrongdoing.

183. Path thus knowingly and intentionally accessed, copied, uploaded, transmitted to its servers, used, and remotely stored its users' private address books that they maintained on their iDevices, including those of the Plaintiffs.

184. Path's collection and storage of user address books also violated Path's own pre-February 2012 announced policies and the App store guidelines, which for example prohibit "scraping" any user iDevice data without asking.

185. Additionally, Morin inexplicably contended that Path's theft of users' address materials was "industry best practice," which was not true. *Cryptographic hashing* could securely and privately anonymise private data but still allow matching and was well known to app developers and Apple.

186. Nonetheless, Path wrongfully obtained Plaintiffs' private address books by causing an unauthorized call to be made by Plaintiffs' iDevices, following which the iDevice and App would then upload and transmit bulk portions of the Plaintiffs' address book materials via Wi-Fi, 3G and the Internet to Path's servers, where Path then remotely stored and used the materials, all without asking Plaintiffs first or obtaining their consent. In the process, Path has wrongfully obtained, disclosed and de-privatized the Plaintiffs' valuable private address books. On information and belief, these actions re-occurred when Plaintiffs and other Path users re-launched or updated the Path App, which Plaintiffs did several times after they registered up through February 6, 2012.

187. At no point before February 6, 2012 did Path ever ask Plaintiffs if they could do any of these things.

188. Plaintiffs recall no warning or notice from Path or its App, and did not consent to Path's surreptitious conduct.

189. On information and belief, Plaintiffs' address book materials also were not uploaded in a reasonably secure manner from Plaintiffs' iDevices by Path's App or stored in a reasonably secure manner on Path's servers.

190. On information and belief, Path stored and used the address book data obtained from Plaintiffs' and other Path users' iDevices.

191. Unlike Apple, Google did not permit a Path App with such surreptitious address book harvesting functions to infest its app marketplace or onto Android wireless mobile devices. In fact, the Android version of the Path App requested permission to upload Android owners' address books before doing so.

192. On information and belief, Path has modified the Path App to display an opt-in alert and notification screens "before any upload of user address book materials could occur so that user privacy is "protected. " Path issued this modified App release and it was made available on the App Store on February 8, 2012. The alert it issued, notified users contacts would be sent to its servers but did not hash the data.

> "**Contacts** To find family and friends, Path needs to send your contacts to our server" [Don't allow] [OK]"

is inaccurate and deceptive

193. Not until April 2, 2012 did Path announce that its App would start "hashing user contact data" to "protect user privacy."

194. Accordingly, Path appears to now recognize that both prior notification and hashing is ***essential*** to adequately protect iDevice users' privacy and their address books, and to comply with acceptable industry and Apple mandated standards.

195. On information and belief, Path was aware of the present lawsuit before making these modifications to its App.

Like Path, the other Application Developer Defendants appropriated and misused their App users' private wireless mobile device Address Book Data

196. Myriad technical blogs and news reports posted assessments and articles describing numerous Apps that without the iDevice user's prior informed consent appeared to access, copy, transmit, upload, obtain possession of, use and/or remotely store partial or full copies of the App user's private Address Book Data that the user maintains on his or her wireless mobile device.

Hipster

197. Defendant Hipster authored the Hipster App, with Apple providing assistance through the iOS Developer Program and a digital certificate for the App to function on iDevices.

198. Plaintiff Rachelle King recalls navigating to various screens on and using the Hipster App. More particularly, she recalls navigating within the Hipster App to a "Find Friends" menu screen containing an option labeled "Contacts."

199. Plaintiff King does not recall being presented at any time in that process or before downloading or launching the Hipster App with an alert or warning indicating that the Hipster App would upload his or her address book to Hipster or anyone else.

200. Published reports, including those from a computer engineering professor, indicate that before February 11, 2012, when an iDevice Hipster App user opened the App's "Find Friends" menu (but before the user even had a chance to select the "Contacts" option on that screen), the iDevice would, without first asking or securing consent, initiate in the background a call, copy the iDevice owner's address book's complete set of email addresses, and the iDevice would then upload and transmit those materials in plain-text, unencrypted via an unsecure HTTP GET via Wi-Fi, 3G and the Internet to Hipster's servers, where Hipster then remotely used and stored the materials. On information and belief, this happened to Plaintiffs who had the App and re-occurred when the App was re-launched. Upon information and belief,

this occurred to Plaintiff when she registered for Hipster. Hipster did not disclose this would occur.

201. Accordingly, Hipster wrongfully and intentionally obtained, retained, disclosed and de-privatized these Plaintiffs' valuable private address books and used their iDevices without authorization. Hipster and its App never asked Plaintiffs if they could do any of these things and never alerted or informed Plaintiffs that these actions were occurring. Hipster did this solely for its financial benefit and harmed its users, including Plaintiffs.

202. In a February 8, 2012, Hipster CEO Doug Ludlow acknowledged and apologized for the Hipster App uploading its users' Address Book Data, conceding that "***we [Hipster] clearly dropped the ball when it comes to protecting our users' privacy***."

203. Hipster also admitted that its conduct did not meet its standards for the protection of [its'] user's data."

204. Following this, Hipster issued a modified version of its App, which added alerts that clearly indicated what would occur.

Foursquare

205. Defendant Foursquare Labs authored the *Foursquare* App, with Apple providing assistance through the iOS Developer Program and a digital certificate for the App to function on iDevices. Following Apple's review, Apple released, distributed and marketed the *Foursquare* App on the App Store.

206. The identified Plaintiffs recall signing up and logging in on the *Foursquare* App's sign-up/log-in screen prior to February 2012 and then using and navigating around the App.

207. Plaintiffs do not recall being presented either then, before downloading or before launch of the *Foursquare* App with an alert or warning indicating that the *Foursquare* App would upload Plaintiff's address book to Foursquare Labs or anyone else.

208. Published reports state that when a user, like Plaintiffs, signed up, without warning or a request for consent, the *Foursquare* App uploaded all email addresses and phone numbers in the iDevice owner's address book. On information and belief, the owner's iDevice initiated an unauthorized call and then uploaded and transmitted those materials in-bulk via Wi-Fi, 3G and the Internet to unintended recipient Foursquare Lab's servers, where Foursquare Labs then remotely stored and used the materials. This happened to Plaintiffs and, on information and belief, re-occurred on more than one occasion.

209. As determined in an analysis by *Tapbot* App founder Paul Haddad,

> "Foursquare [ ] was uploading all of the email addresses and phone numbers in [a user's] address book with no warning and no explicit consent given ."
>
> "Foursquare also seems to be sending out phone numbers for contacts as well. This is on launch, after creating a new account."
>
> "Foursquare 4.2 (latest), Sends out all email address in address book via HTTPS, no warning, no hashing."

210. Foursquare Labs' communications director also verified in press e-mails that it "*transmit[ted] the address book information*."

211. Prior to February 6, 2012, the "Connect with your friends" screen in the *Foursquare* App itself would display how many of the user's "contacts are on foursquare" because it had already uploaded the user's address book by then.

212. Accordingly, Foursquare Labs has wrongfully obtained, retained, disclosed and de-privatized these Plaintiffs' valuable private address books and used their iDevices without

authorization. Foursquare Labs and its App never asked Plaintiffs if they could do any of these things.

213. On information and belief, the Plaintiffs' address book was not hashed to protect its anonymity before being transmitted to Foursquare Labs' servers.

214. Following February 2012 news reports on its App's address book harvesting issue, Foursquare Labs modified its App to include the following programmatic halt and pop-up alert:

> "**Searching for friends who are using foursquare?** To find your friends, we send your address book information to our servers. Don't worry, it's sent securely and we don't store it! [Noooo!] [Ok]"

Instagram

215. Defendant Instagram, on information and belief, owns and authored the Instagram App, with Apple providing assistance through the iOS Developer Program and a digital certificate to for the App to function on iDevices. Following Apple's review, Apple released, distributed and marketed the Instagram App on the App Store. The App Store and Apple's accompanying iTunes page shows Defendant Burbn holding the copyright in and being the "seller" of the Instagram App and titles the App "Instagram by Burbn, Inc."

216. The identified Plaintiffs recall using and navigating around the Instagram App.

217. One or more of the identified Plaintiffs recalls signing in, navigating within the Instagram App to a "Find friends" screen, tapping a displayed "From my contact list" button bar, and then being presented with a list of recognizable names that the Plaintiff could choose to "follow" by pressing another button near each name.

218. Plaintiffs do not recall being presented at the time with any intervening alert or pop-up dialogue box warning them that their address book had to or would be transmitted to Instagram to perform this function.

219. Published reports that included *mitmproxy* tool data flow analysis screenshots showed that when Instagram App users tapped the "From my contact list" button bar, the owner's iDevice initiated an unauthorized call and transmitted in-bulk, unencrypted, and in plain text to Instagram's (or, possibly, Burbn's) servers the first names, last names, email addresses and phone numbers from the user's iDevice address book.

220. On information and belief, Instagram and Burbn, via the Instagram App, caused Plaintiff's iDevice to initiate an unauthorized call and upload, remotely use and store extensive bulk portions of Plaintiffs' address books, without Plaintiffs' consent. Instagram has wrongfully obtained, retained and de-privatized Plaintiffs' valuable private address books. Neither Instagram, Burbn nor the Instagram App Instagram ever asked Plaintiffs if they could do this. Plaintiffs never consented to the taking or transmission of their address books. Plaintiffs never consented to bulk lists of email addresses, phone numbers, contact names or other fields of data in their iPhone's Address Book Data being uploaded and transferred to Instagram's (or any other person's) servers or to that data being used, manipulated or stored other than on his or her iPhone.

221. On information and belief, the Plaintiffs' address book was not hashed to protect its anonymity before being transmitted to Instagram's servers.

222. These Plaintiffs recall no warning or notice from Instagram, Burbn, Apple or the App Store that the Instagram App and iDevice would be transmitting and Instagram (or Burbn) would be taking, receiving, using and storing any portions of his or her address book.

223. In mid-February 2012, ***after*** media reports about similar unauthorized address book harvesting, a revised version of the Instagram App was quietly issued that included a programmatic halt and the following pop-up alert that appeared when a user tapped the "From my contacts list" button bar on the "Find Friends" page:

> "**Search for Your Friends in Address Book?** In order to find your friends, we need to send address book information to Instagram's servers using a secure connection. [Cancel] [Allow]."

The statement in this alert is not even true. Instagram could easily elect to use anonymized hashed data to blind match users "friends" without ever needing any of the raw address book materials.

224. Instagram has agreed to be acquired by co-defendant Facebook. The acquisition is currently pending regulatory approval.

Yelp!

225. Defendant Yelp authored the Yelp! App, with Apple providing assistance through the iOS Developer Program and a digital certificate for the App to function on iDevices. Following Apple's review, Apple released and distributed the Yelp! App on the App Store.

226. The identified Plaintiffs each recall navigating to various screens on and using the Yelp! App. More particularly, they recall providing a log in and navigating within the Yelp! App to a screen containing a ["Find Friends"] button with the accompanying displayed text:

> "Find friends on Yelp using your Contacts and Facebook friends? You'll be able to see their bookmarks and find out when they're nearby. [Yes, Find Friends] [No, Skip This]",

and pressing the ["Yes, Find Friends"] button. Plaintiffs do not recall being presented at any time in that process with an intervening alert or pop-up display indicating that the Yelp! App would

upload his or her address book to Yelp to perform this function or warning that such a transmission was about to occur.

227. The displayed Yelp! App text does not request permission to upload any address book materials from Plaintiffs' iDevices or transmit any address book material off of Plaintiffs' iDevices.

228. Published reports indicate that before February 2012 when an iDevice Yelp! App user tapped the ["Yes, Find Friends"] button, the iDevice would, without first asking or securing consent, initiate a call, copy bulk portions of the user's address book, and the iDevice would then upload and transmit those materials via Wi-Fi, 3G and the Internet to Yelp's servers, where Yelp then remotely stored, used and kept the materials. This occurred to Plaintiffs multiple times.

229. Accordingly, Yelp has wrongfully obtained, retained, disclosed and de-privatized these Plaintiffs' valuable private address books and used their iDevices without authorization. Yelp and its App never asked Plaintiffs if they could do any of these things.

230. Following adverse media reports like the TIMES article, Yelp modified its App in mid-February 2012 so that it now halts and an alert appears when a user taps the ["Find Friends"] button that reads:

> "**Find Friends** To find friends, we'll need to upload your contacts to Yelp. Don't worry, we're not storing them. [No Thanks] [OK]"

Twitter

231. Defendant Twitter authored the Twitter App, with Apple providing assistance through the iOS Developer Program and a digital certificate for the App to function on iDevices. Following Apple's review, Apple released and distributed the Twitter App on the App Store.

232. The identified Plaintiffs each recall opening the Twitter App, signing up via its displayed registration screen, and using the App. More particularly, they recall being presented a

"**Welcome**" screen prompting them to press an on-screen button labeled ["Follow your friends"], under which was written in small type: "Scan your contacts for people you already know on Twitter." They also recall another screen labeled "Follow Friends" that similarly prompted them to press an on-screen button labeled ["Follow your friends"], under which was written in small type the identical phrase as before.

233. The App's ["Follow your friends"] button-bar and accompanying texual phrase do not constitute a request for permission to upload any address book materials from Plaintiffs' iDevices or transmit any address book material off of Plaintiffs' iDevices.

234. As prompted, prior to February 2012, each Plaintiff pressed the displayed ["Follow your friends"] button-bar. Plaintiffs recall no alerts or warnings that their address books were being taken.

235. According to Twitter, prior to February 2012, when Twitter App users tapped the ["Follow your friends"] button-bar, their iDevice silently made a call over the internet and the Twitter App then uploaded all email addresses and phone numbers from the iDevice owner's address book to Twitter's servers, where Twitter used, stored and planned to keep those materials for up to eighteen months, likely in unsecure plain text. This occurred to Plaintiffs.

236. Accordingly, Twitter has wrongfully obtained, retained, disclosed and de-privatized Plaintiffs' valuable private address books. Twitter and its App never asked Plaintiffs if they could upload and store their address book. Thus, consent was never given to do so.

237. After media questioned Twitter's App privacy practices and secret address book collection, sometime after February 6, 2012 Twitter modified the language on its Twitter App's "Find Friends" screen and ["Follow your friends"] button, replacing the phrase "***scan*** your contacts" with the phrase "***upload*** your contacts" and also added the following intervening alert:

> "**Find Friends on Twitter** We will securely upload your contacts to help you find friends and suggest users to follow on Twitter. [Cancel] [OK]"

Foodspotting

238. Defendant Foodspotting authored the Foodspotting App, with Apple providing assistance through the iOS Developer Program and a digital certificate or the App to function on iDevices. Following Apple's review, Apple released, distributed and marketed the Foodspotting App on the App Store. The identified Plaintiffs recall opening the Foodspotting App, signing up via its registration screen, and using the App. More particularly, they recall navigating to the Foodspotting App's "**Follow People**" screen containing an on-screen button labeled ["Find iPhone Contacts."]. While on that screen, Plaintiffs tapped that button. The screen contained no warnings whatsoever indicating that the App was uploading his or her address book to Foodspotting.

239. The displayed button and screen menu name do not constitute a request for permission to upload any address book materials from Plaintiffs' iDevices or transmit any address book material off of Plaintiffs' iDevices and Plaintiffs did not consent to this.

240. According to defendant Foodspotting's February 15, 2012 company blog, when App users tapped the ["Find iPhone Contacts]" button, the iDevice would, silently and without first asking or securing consent, initiate a call, copy bulk portions of the user's address book (in particular, all email addresses), and the iDevice would then upload and transmit those materials via Wi-Fi, 3G and the Internet to Foodspotting's servers, where Foodspotting then remotely used and stored the materials. Upon information and belief, this occurred to Plaintiffs multiple times. Reports indicate the transmission was insecure and included the user's "unencrypted address book data [… with] a list of email addresses in plain text."

241. Accordingly, Foodspotting has wrongfully obtained, retained, transmitted, disclosed and de-privatized these Plaintiffs' valuable private address books and used their iDevices without authorization. Foodspotting and its App never asked Plaintiffs if they could do any of these things.

242. Following adverse media reports, Foodspotting announced it had "address[ed] address book concerns" in its modified App by adding "extra permissions and security," including a new pop-up alert/dialogue box to its App's "Follow People" page and ["From iPhone Contacts"] button. Foodspotting reportedly updated its App at that time to also employ HTTPS transmissions.

Angry Birds Classic/Crystal - Rovio & Chillingo

243. Defendant Rovio authored the *Angry Birds Classic* App.

244. On information and belief, integrated into the *Angry Birds Classic* App available over the App Store is Chillingo's *Crystal* platform, which, on information and belief, is an App itself. On information and belief, Chillingo's *Crystal* platform is integrated, either by Chillingo or the game developer, into many gaming Apps offered on the App Store.

245. On information and belief, either (a) Chillingo first licenses the *Angry Birds Classic* App from Rovio, integrates the *Crystal* platform into it and then releases it through Chillingo on the App Store, (b) Rovio integrates the *Crystal* platform into its own App, which it self-releases on the App Store, or (c) Chillingo and Rovio work together to release an App containing both the *Angry Birds Classic* and *Crystal* features.

246. Apple provides assistance through the iOS Developer Program and a digital certificate for the *Angry Birds Classic* App (and, possibly, the *Crystal* platform) to function on iDevices. Following Apple's review, Apple released, distributed and marketed the integrated

Angry Birds Classic App on the App Store. The *Angry Birds Classic* App is available in both free and paid versions on the App Store.

247. The identified Plaintiffs recall opening the *Angry Birds Classic* App, playing some games of Angry Birds, and navigating around to other screens and menus within the App. More particularly, one or more Plaintiffs recall after signing up on the integrated *Crystal* platform navigating within the *Angry Birds Classic* App to the "Send an invite" screen (with the subheading "Invite your friends to Angry Birds"), and pressing the button bar labeled "Invite from contacts" with the subheading "Send an invite from your local Contacts." Plaintiffs do not recall being presented at any time in that process with an intervening alert or pop-up display indicating that the App (or Apps) would upload his or her address book to perform this function or warning that such a transmission was about to occur.

248. The displayed in-App text does not request permission to upload any bulk address book materials from Plaintiffs' iDevices or transmit any bulk address book material off of Plaintiffs' iDevices.

249. Published reports containing *mitmproxy* data-flow screen shots indicate that before February 2012 when an iDevice *Angry Birds Classic* App user tapped the ["Invite from contacts"] button, the iDevice would, without first asking or securing consent, initiate an unauthorized call, copy bulk portions of the user's address book, and the iDevice would then upload and transmit those materials via Wi-Fi, 3G and the Internet to one or both companies' servers, where they remotely stored and used the materials. On information and belief, this happened to Plaintiffs multiple times. On information and belief, these functions may have been enabled by App components provided by Chillingo.

250. On information and belief, the non-consensually uploaded user address book materials were transferred to Rovio's and/or Chillingo's computer servers. On information and belief, the uploaded user address book materials were also transferred to other third parties, including Chillingo (operator of the Crystal gaming network), and reportedly may also have been transferred to Google.

251. Accordingly, Rovio and/or Chillingo have wrongfully obtained, retained, disclosed and de-privatized these Plaintiffs' valuable private address books and used their iDevices without authorization. Rovio and Chillingo (and their Apps) App never asked Plaintiffs if they could do any of these things.

252. Rovio represents that "No contact information is collected or stored by Crystal." On information and belief, that statement is not true.

253. Before February 2012, Rovio and Chillingo never notified the identified Plaintiffs that the integrated *Angry Birds Classic* App would make an unauthorized call on their iDevices or upload in bulk or transmit any of their address book materials to a remote location. Nor did Chillingo.

254. Before February 2012, Rovio never notified the identified Plaintiffs that Rovio or any other third party would be manipulating or using any of their Address Book Data at a remote location. Nor did Chillingo.

255. On information and belief, in mid-February 2012 (i.e., ***after*** reports and privacy concerns surfaced about Apps violating their users' privacy), either Rovio or Chillingo added a new alert box to the integrated *Angry Birds Classic* App's "Send an invite" screen that included language stating that pressing that button would cause the "upload" of the user's Address Book Data to Rovio's or another party's computer server.

Cut the Rope - ZeptoLab, Chillingo & Electronic Arts

256. On information and belief, Defendant ZeptoLab authored the *Cut the Rope* App.

257. Chillingo is identified on Apple's iTunes Cut the Rope page as "publisher" of the Cut the Rope App.

258. On information and belief, integrated into the *Cut the Rope* App available over the App Store is Chillingo's *Crystal* platform, which, on information and belief, is an App itself.

259. On information and belief, either (a) Chillingo first licenses the *Cut the Rope* App from ZeptoLab, integrates the *Crystal* platform into it and then releases it through Chillingo on the App Store, (b) ZeptoLab integrates the *Crystal* platform into its own App, which it self-releases on the App Store, or (c) Chillingo and ZeptoLab work together to release an App containing both the *Cut the Rope* and *Crystal* features.

260. Apple provides assistance through the iOS Developer Program and a digital certificate for the *Cut the Rope* App (and, possibly, the *Crystal* platform) to function on iDevices. Following Apple's review, Apple released, distributed and marketed the integrated *Cut the Rope* App on the App Store. The *Cut the Rope* App is available in both free and paid versions on the App Store.

261. The identified Plaintiffs recall opening the *Cut the Rope* App, playing some games of Cut the Rope, and navigating around to other screens and menus within the App. More particularly, one or more Plaintiffs recall after signing up on the integrated *Crystal* platform navigating within the *Cut the Rope* App to the "Find friends" screen and pressing the button bar labeled ["Find friends via contacts"].

262. Plaintiffs do not recall being presented at any time in that process with an intervening alert or pop-up display indicating that the App (or Apps) would upload his or her address book to perform this function or warning that such a transmission was about to occur.

263. The displayed in-App text does not request permission to upload any bulk address book materials from Plaintiffs' iDevices or transmit any bulk address book material off of Plaintiffs' iDevices.

264. Publishing reports indicate that before February 2012 when an iDevice *Cut the Rope* App user tapped the ["Find friends via contacts"] button, the iDevice would, without first asking or securing consent, initiate an unauthorized call, copy bulk portions of the user's address book, and the iDevice would then upload and transmit those materials via Wi-Fi, 3G and the Internet to one or both companies' servers, where they remotely stored and used the materials. On information and belief, this happened to Plaintiffs multiple times. On information and belief, these functions may have been enabled by App components provided by Chillingo.

265. On information and belief, the non-consensually uploaded user address book materials were transferred to ZeptoLabs' and/or Chillingo's computer servers. On information and belief, the uploaded user address book materials were also transferred to other third parties and reportedly may also have been transferred to Google.

266. Accordingly, ZeptoLab and/or Chillingo have wrongfully obtained, retained, disclosed and de-privatized these Plaintiffs' valuable private address books and used their iDevices without authorization. ZeptoLab and Chillingo (and their Apps) App never asked Plaintiffs if they could do any of these things.

267. Plaintiffs do not recall being presented at any time in that process with any alert or notification stating that any of their address book materials would be uploaded from his or her iDevice to ZeptoLab's, Chillingo's or any other third parties' computer servers.

268. Plaintiffs were never informed and never consented to bulk portions of their iDevice address book materials being uploaded and transferred to ZeptoLab's, Chillingo's (or any other person's) servers or to that data being possessed by others or remotely used or manipulated off of the device or remotely stored.

269. On information and belief ZeptoLab and Chillingo have engaged in these actions with the assistance, support, encouragement and/or direct material participation of the other and/or Electronic Arts.

270. On information and belief, sometime around February 17, 2012 (i.e., ***after*** reports and privacy concerns surfaced about Path violating its users' privacy by uploading portions of their address books to Path's servers without the users' authorization), ZeptoLab (or Chillingo) added a new alert box to the Cut the Rope App stating that activation of the "find friends" feature would result in the "upload" of the user's Address Book Data to ZeptoLab's or another party's computer server.

271. On information and belief, Chillingo was recently acquired by and now is a division of Electronic Arts. On information and belief, Electronic Arts is a successor-in-interest to Chillingo's obligations and liabilities. Consequently, on information and belief, ZeptoLab, Chillingo and Electronic Arts are jointly and severally liable on the claims alleged herein pertaining to the Cut the Rope App.

Electronic Arts

272. On information and belief, Electronic Arts acquired Chillingo around October 2010 and, according to Electronic Art releases, has operated Chillingo as a division of Electronic Arts since the acquisition.

273. On information and belief, Electronic Arts is a successor-in-interest to Chillingo's obligations and liabilities.

274. Consequently, on information and belief, ZeptoLab, Chillingo and Electronic Arts are jointly and severally liable on the claims alleged herein pertaining to the *Cut the Rope* App and Chillingo and Electronic Arts are jointly and severally liable on the claims alleged herein pertaining to the *Angry Birds Classic* App.

Facebook

275. During the pendency of this matter, co-defendants Facebook and Instagram announced in April 2012 an agreement for Facebook to acquire Instagram for $300 million in cash and 23 million shares of Facebook stock. That acquisition closed on September 6, 2012.

276. On information and belief, Facebook acquired Gowalla (and/or its assets and/or key employees) for an undisclosed sum in December 2011. On information and belief, Facebook made payments of cash and/or Facebook pre-IPO stock either to Gowalla or to Gowalla's stockholders in consideration for this transaction.

277. On information and belief, from its pre-acquisition due diligence of Gowalla (and well as its acquisition of Beluga, an App developer who's App had similar address book functionalities), Facebook was aware of the *Gowalla* App's surreptitious user-address-book upload functionalities discussed above.

278. After the Facebook acquisition, Gowalla continued to offer the *Gowalla* App to the public for approximately three more months until approximately March 12, 2012. On information and belief, this activity was authorized, approved, managed and/or directed by Facebook, despite the risk of harm from continued distribution of this App. Facebook eventually shuttered the Gowalla service and App around March 12, 2012.

279. Accordingly, for the periods subsequent to Facebook's acquisition of Gowalla, on information and belief Facebook knowingly aided and abetted Gowalla in the commission of its wrongful activities described above and, consequently, is jointly and severally liable to the Plaintiffs on each of the claims and for all of the harm and damages described herein pertaining to Gowalla during those periods.

280. Also, on information and belief, Facebook's acquisition of Gowalla and/or substantially all of Gowalla's staff, assets and operation was for less than equivalent value and via a transaction designed to improperly shield assets from Gowalla's prospective creditors. On information and belief, with Facebook's authorization and assistance and the cooperation of Gowalla and its management, without satisfying or reserving for all creditor claims Gowalla distributed substantially all consideration received from Facebook – which at the time was the predominant remaining assets of the business—to its equity-holders for less than equivalent value, in violation of the Uniform Fraudulent Transfer Act, and in a manner that left Gowalla insolvent. Accordingly, Facebook is Gowalla's successor-in-interest and is liable on the claims asserted against Gowalla in this action and the wrongfully distributed assets should be impressed with a constructive trust.

281. Accordingly, Facebook is a successor-in-interest to Gowalla's obligations and liabilities and is liable on each claim asserted herein against Gowalla as its successor-in-interest.

Burbn

282. On information and belief, Burbn is a predecessor-in-interest to Instagram and is identified on the App Store as the publisher or intermediary source of the Instagram App. On information and belief, Instagram is also either a successor-in-interest to the business of Burbn or is related to or affiliated with Burbn.

283. Plaintiffs were harmed by the Defendants' acts described above.

284. Defendants have benefited and were unjustly enriched by their wrongful acts.

285. Defendants' acts alleged herein were willful, intentional, knowing and malicious.

286. Defendants' acts alleged herein were reckless.

287. Because of the surreptitious nature of their actions, only Defendants know exactly what was stolen, when, and how:

288. On information and belief, the Plaintiffs' address books materials were not hash to protect Plaintiff's privacy in advance of the unauthorized transmissions and uploads discussed above; not are they now for the App Defendants.

289. The Uploads and transmission constitute "electronic communications."

290. The App Defendants exceeded any authorized access when they committed the acts above.

291. Defendants' acts and wrongful conduct will continue unless enjoined by the Court.

292. Plaintiffs have no adequate remedy at law.

CAUSES OF ACTION

A. COMMON LAW CLAIMS

1. INVASION OF PRIVACY

293. Plaintiffs incorporate the preceding paragraphs and further allege:

294. Plaintiffs have a reasonable expectation in the privacy for their iDevices and their address books.

295. The App Defendants intentionally intruded on Plaintiff's solitude, seclusion or private affairs by uploading, copying, reviewing, disclosing, storing, and disseminating their private address books. Defendant's intrusion was highly offensive to a reasonable person. As a direct and proximate result, Plaintiffs suffered damages.

296. Moreover, the private affairs of the Plaintiffs include their address books and the contents of their iDevices and their private address books and unique contacts. These are not matters of legitimate public concern.

297. As a consequence of the App Defendants' conduct, this information was taken and publicly disclosed, and Plaintiffs suffered damages.

2. COMMON LAW MISAPPROPRIATION

298. Plaintiffs incorporate the preceding paragraphs and further allege:

299. The App Defendants intentionally and willfully appropriated, either in whole or in part, bulk portions of each Plaintiff's iDevice's private address book.

300. Plaintiffs expended substantial time and effort collecting the contacts in, and over time assembling, their address books.

301. On information and belief, each App Developer has (via its respective Apps) automatically, secretly, and with little effort harvested and swept into their computers systems and social and data networks some or all of the fields from Plaintiffs' private address books and used those materials for their own purposes and to their own benefit.

302. On information and belief, the App Developers' respective Apps periodically re-accessed or re-sent their users' iDevices' address books or information thereof.

303. Thus, the App Defendants have impermissibly mined their App users' iDevices for contacts data, thereby obtaining an unjustified and inequitable free ride on and benefit from Plaintiffs' prior efforts.

304. As a direct and proximate result, Plaintiffs have suffered damages.

3. CONVERSION

305. Plaintiffs incorporate the preceding paragraphs and further allege:

306. Plaintiffs have the immediate right to possession of, ownership of and/or title to their address books and iDevices, which constitute personal property. Plaintiffs' rights are superior to those of any Defendant.

307. As described herein, the App Developers have each wrongfully exercised dominion or control over at least a portion of the Plaintiffs' address books and iDevices to the exclusion of, or inconsistent with, Plaintiffs' rights of exclusive possession and control.

308. As a direct and proximate result, Plaintiffs have sustained damages.

4. TRESSPASS TO PERSONAL PROPERTY AND/OR CHATTELS

309. Plaintiffs incorporate the preceding paragraphs and further allege:

310. Plaintiffs' iDevices and address books constitute chattel and personal property.

311. The App Defendants have each wrongfully and intentionally and without consent intermeddled with Plaintiffs' iDevices and their address books.

312. The App Defendants have each wrongfully and intentionally interfered with Plaintiffs' possession and use of their iDevices and their address books as discussed above. The intermeddling and interference was conducted surreptitiously and without authorization of Plaintiffs.

313. These Defendants' acts impaired the condition, use, value and quality of Plaintiffs' iDevices and their address books and proximately caused Plaintiffs to suffer damages.

5. MISAPPROPRIATION OF TRADE SECRETS AND PROPRIETY INFORMATION

314. Plaintiffs incorporate preceding paragraphs and further allege:

315. Plaintiffs use reasonable efforts, under the circumstances, to maintain the privacy and secrecy of their iDevice address books.

316. Plaintiffs' address books are compilations of information that substantial efforts went into assembling and creating.

317. Plaintiffs address books have value and have independent economic value from not being generally known by others or readily ascertainable by proper means.

318. The App Defendants obtained, disclosed, and used Plaintiffs' proprietary address books or portions thereof without Plaintiffs' express or implicit consent.

319. The App Defendants obtained Plaintiffs' address books or portions thereof by improper means.

320. Plaintiffs were harmed by Defendants appropriation of their address books.

321. Defendants benefitted, profited, and were unjustly enriched by their wrongful appropriation and use of Plaintiffs' address books.

322. Plaintiffs are entitled to their actual damages, including, at Plaintiffs' elections, a reasonable royalty, Defendants' unjust enrichment disgorgement.

323. Defendants' acts were willful and malicious. Accordingly, Plaintiffs are entitled to exemplary damages.

324. Defendants' use of materials gleaned from address books will continue unless enjoined by the Court.

325. Accordingly, Plaintiffs' are entitled to injunction.

6. NEGLIGENCE

- **As to the App Defendants**

326. App Defendants violated criminal law and general standards of care by putting out malware that invades user privacy.

327. The App Defendants breached the duty of care owed to Plaintiffs and their users by, among other things.

- Violating the criminal law, particularly California Penal Code §502, The Texas Computer Security Act, Texas Penal Code §33.02, 16.02 and other criminal statutes cited herein
- Failing to operate according to industry accepted standards with regard to mobile device privacy and security.

328. As a direct and proximate result, Plaintiffs suffered damages.

- **As to Apple**

329. Apple was negligent as it:

- Failed to conduct rigorous reviews as promised;
- Failed to protect Plaintiffs' and consumers' privacy, particularly with regard to their address books, as promised;
- Failed to warn Plaintiffs and consumers about malicious Apps it distributed and known iDevice security risks;
- Failed to correct multiple misrepresentation concerning privacy protection and iDevice security.
- Failed to meet common industry standards relating to iDevice privacy and security.

330. As a direct and proximate result, Plaintiffs suffered damages to their person and property.

331. Plaintiffs' damages include, *inter alia*, reasonable expenses for each Plaintiff to remedy and prevent the security breaches exposed by the App Defendants' wrongful conduct, recoupment of the value of the address books appropriated from their iDevices and the de-privatization of those materials, and other economic and noneconomic harm—for which they are entitled to compensation.

332. Defendants' wrongful actions and/or inaction (as described above) constitute negligence at common law, negligence *per se*, negligence and gross negligence.

B. STATUTORY CLAIMS UNDER FEDERAL LAW

1. INTERCEPTION OF ELECTRONIC COMMUNICATION UNDER THE ELECTRONIC COMMUNICATION PRIVACY ACT ("ECPA")

333. Plaintiffs incorporate the preceding paragraphs and further allege:

334. Each Defendant is a "person" within the meaning of § 2511.

335. Each App Defendant's respective App (and any components provided by Chillingo) used to transfer information constitutes alone and in combination with an iDevice an "electronic device" under 18 U.S.C. § 2510(5) and all other relevant federal and state statutes cited herein.

336. Each Plaintiff's sending of address book materials to his or her iDevice from another computer via the electronic "syncing" process constitutes an "electronic communication" within the meaning of 18 U.S.C. § 2510(12), as does any subsequent transmission or upload of any portion of the address book materials from the iDevice.

337. In no event was any App Defendant an intended recipient of Plaintiff to any unintended and unauthorized calls initiated by their iDevices. They were not intended recipients of any such communications. On information and belief, and as alleged herein, each Defendant has without authorization intentionally intercepted electronic communications that contained some or all of the address book materials from users' iDevices, and has intentionally made use of the content of such communications. On information and belief, one or more of the Defendants have also without authorization subsequently disclosed to others the contents such intercepted communications—such as through the s disclosure of sale of assembled contact lists—in violation of 18 U.S.C. § 2511(c).

338. On information and belief, each such defendant knew or had reason to know that the information was obtained through the interception of a wire or electronic communication in violation of this statute.

339. Accordingly, each Plaintiff is a "person whose . . . electronic communication [was] intercepted, disclosed or intentionally used in violation of this chapter" within the meaning of 18 U.S.C. § 2520.

340. The Plaintiffs have been directly harmed and suffered actual damages as a result of the App Defendants' violations of the Electronic Communications Privacy Act, each of whom have benefited and profited as a result of their respective violations.

341. On information and belief, the App Defendants and have repeatedly and routinely violated the Electronic Communications Privacy Act in this manner using their respective Apps.

342. Accordingly, each Plaintiff is entitled to recover from each corresponding Defendant ***the greater of***: (i) his or her actual damages plus any Defendant's profits realized

from the use of Plaintiffs' address book materials; or (ii) statutory damages of the greater of $10,000 apiece or $100 a day for each day of violation.

343. Plaintiffs are also entitled to recover reasonable attorneys' fees and other litigation costs.

2. 18 U.S.C. §1030(G)
FRAUD IN CONNECTION WITH COMPUTERS

344. Plaintiffs re-allege the above paragraphs.

345. Plaintiffs' devices are "protected computers."

346. The aggregate lost in any one-year period exceeds $5,000.

347. Defendants' acts and the unauthorized address book transmissions jeopardized public security and computers owned or used by the government in furtherance of justice, defense, or security.

348. On the basis of the Defendants' above alleged actions, the App Defendants have each violated the requisite sections of 18 U.S.C. § 1030 so as to subject them under 18 U.S.C. § 1030(g) to civil liability and to permit recovery in a civil action by any person who suffers damage or loss by reason of the violation.

349. Plaintiffs have suffered damage and/or loss by reason of each of these Defendants' violations of 18 U.S.C. § 1030.

350. Accordingly, Plaintiffs seek recovery of their compensatory damages as authorized under 18 U.S.C. § 1030(g), including: (i) reasonable costs for validating the integrity of the Plaintiffs' address books and/or restoring such address books to the condition they were in before the Defendants' respective offenses; (ii) costs for appropriate additional security measures on the Plaintiffs' iDevices to remedy the address books-related security flaws that the Defendants exposed and to inhibit and prevent similar offenses in the future; (iii) the reasonable

costs for each Plaintiff to conduct or have conducted a detailed damage and integrity assessment of his or her iDevice and the address books maintained thereon and to assess whether the address books and/or its availability or accessibility or the iDevice device has been impaired in any way; and (iv) the value and costs of the wireless airtime that those Apps caused to be consumed while surreptitiously uploading any portion of a Plaintiff's address books from his or her iDevice.

351. On information and belief, these App Defendants' conduct has been intentional and willful in nature.

352. As described herein, each of these defendants inserted code into their Apps that surreptitiously harvested Plaintiffs' address books. Based on Apple's review process, and other insight Apple also knew about this.

353. These Defendants had no authorization to take or store this valuable information, and each acted intentionally.

354. As a consequence, Plaintiffs and potential class members, have suffered aggregate losses in a one year period - from the time of each unauthorized uploading, above $5,000

3. RICO VIOLATIONS UNDER 18 U.S.C §§1961-1964

355. Plaintiffs re-allege the above paragraphs.

356. Violations of 18 U.S.C. §§ 1343 and 2314 are predicate acts under the Racketeering Influence & Corrupt Organizations Act (18 U.S.C. § 1962, et seq.). *See* 18 U.S.C. §§ 1961(1). Each App Defendant is alleged above to have committed both of these predicate acts.

Wire Fraud (18 U.S.C. § 1343)

357. The App Defendants obtained bulk portions of Plaintiffs' address books under false pretenses and as part of a scheme to defraud. They also each caused bulk portions of the

Plaintiffs' private address books to be transmitted as electronic signals in interstate commerce by means of wires and the airwaves for the purposes of and in furtherance of executing these schemes. Accordingly, each App Defendants' described actions constitute wire fraud under 18 U.S.C. § 1343.

358. On information and belief, via their acts, each App Defendant has divulged and/or disseminated at least some portion of the contents of Plaintiffs' private address books to: (i) wireless and/or cell phone service providers (*e.g.*, AT&T, Sprint and/or Verizon for iPhone users) through which these materials must pass while in transmission over the internet; (ii) third party server system owners; and/or (iii) their own organizations and their information technology personnel.

Transportation of Stolen Property (18 U.S.C. § 2314 cl.2):

359. Each Application Developer obtained Plaintiffs' and the Class members' property (i.e., bulk portions of their address books) by means of false pretenses under a scheme to defraud. In the aggregate, those materials' value exceeds $5,000. Each App Defendant has transported that data and/or caused that data to be transported in interstate commerce (by, for example, sending it over computer and wireless networks, including the Internet and World Wide Web) in furtherance of their schemes. Accordingly, the Defendants' actions constitute transportation of stolen property in violation of 18 U.S.C. § 2314.

360. On information and belief, once each App Defendant's App was installed on an iDevice, the App functions, in part, to surreptitiously harvest, intercept (and/or cause the interception of), and transmit electronic communications and data and to turn Plaintiffs' iDevice into a relay device and/or bot – i.e. a computer that has been taken over. Accordingly, the App Defendants' Apps constitute "electronic communication intercepting devices" under 18 U.S.C. §

2512 and "computer contaminants" under CAL. PENAL CODE § 502. *See also* TEX. PEN. CODE 16.02(d)(1) (prohibiting the manufacture, sale or distribution of electronic or other devices designed for the nonconsensual interception of wire electronic or oral communications)

Racketeering Influence & Corrupt Organizations (18 U.S.C. § 1962):

361. The App Defendants' wire-tapping activities and transportation of stolen property was facilitated by and committed as described herein with the knowing assistance, encouragement and participation and/or conscious indifference of Apple in contravention of Apple's own standards, policies, agreements, App validation and testing procedures and representations to the consumer market.

362. Each App Defendant in conjunction with Apple conducted or participated in the conduct of the affairs of an enterprise engaged in interstate commerce through a pattern of racketeering activity—here, numerous repeated instances of wire-tapping and transportation of stolen property as well as criminal violations pertaining to Plaintiffs' a personal computers and data—in violation of 18 U.S.C. § 1962(c). Each of the App Defendants, in conjunction with Apple, have formed and participated in an enterprise or association via the App development and approval process and the App Store distribution network and through the affiliation of those companies that are and have been engaged in a pattern of racketeering activities. Moreover, the defendants have pursued the common purpose of making money, gaining market-share, adding persons, nodes and cross-links into their social networks, and expanding their networked databases illegally via the promotion, distribution and sale in interstate commerce of goods and services—*i.e.*, the offending Apps—that have malicious features that automatically and without users' informed consent surreptitiously upload and make use of users' wireless mobile devices and that intercept and take users' personal Address Book Data and similar information in

violation of 18 U.S.C. §§ 1030, 1343 and 2314 (and possibly 2512). Put another way, the App Defendants are using the App Store hierarchy to distribute malware to millions of consumers' iDevice and turns them into zombie bots. This association exists separate and apart from the pattern of racketeering being pursued by these defendants.

363. Each App Defendant conducted or participated in the conduct of the affairs of an enterprise engaged in interstate commerce through a pattern of racketeering activity— in violation of 18 U.S.C. § 1962(c) – here, numerous repeated instances of wire fraud and transportation of stolen property harmful to the Plaintiff, the Class members, and the public. Each App Defendant has formed and participated in enterprises or associations via the social networks each associates with in connection with its App and, in conjunction with Apple, via the App Store's organizational hierarchy and App-development, -verification, -approval, -distribution and -sales network and integrated advertising framework and the affiliation of and between those companies that are and have been engaged in a pattern of racketeering activities. Additionally, the defendants have in combination and collaboration pursued the common purpose of illegally profiting upon, contrary to their own announced policies and contractual obligations via the development, distribution, sale and promotion in interstate commerce of malware (the distributed Apps) that automatically and surreptitiously invaded iDevice owners' privacy, trigger breaches of users' computer security, and stealthily and automatically commit unauthorized disclosures and transmissions in interstate commerce of iDevice owners' private stored electronic communications (i.e., their address book data) in violation of federal and state statutes.

364. Under Apple's oversight and control, the App Defendants altered and impaired owners' iDevices by installing malicious Apps that, in effect, resulted in the iDevices

functioning as bots and illegal electronic eavesdropping and wiretapping devices. The App Defendants' Apps, when combined with a wireless mobile device as intended by both Apple and the App Defendants, surreptitiously capture, relay, and report iDevice owners' private address books to the App Defendants and others. This association exists separate and apart from the pattern of racketeering being pursued by these Defendants. Consequently, Defendants are participating in rings that traffic in, makes use of, and benefit from address book materials taken from the Plaintiffs' iDevices.

365. On information and belief, Apple and the identified App Defendants combined to engage in patterns of racketeering activity in violation of 18 U.S.C. § 1962(d) and engaged in unconscionable, unfair or deceptive practices in or affecting commerce in violation of 15 U.S.C. § 45 that knowingly facilitated and resulted in a stream of technologically-harmful App products coming to market that turn an owner's otherwise functional iDevice into an eavesdropping device that without permission surreptitiously transmits and broadcasts to others the iDevice owner's private address books. The Defendants directly and indirectly receive income and benefits from these patterns of activities.

366. Each App Defendant also directed and controlled the illegal conduct described herein and Apple was involved in and directed and controlled the management of the enterprise itself—the App Store and its associated App development, approval and distribution network.

367. Plaintiffs have been directly harmed as a result of these Defendants' violations of 18 U.S.C. § 1962. Accordingly, Plaintiffs are entitled to recover treble damages and attorneys' fees under 18 U.S.C. § 1964.

368. On information and belief, these Defendants' conduct has been intentional and willful in nature.

C. TEXAS AND/OR CALIFORNIA STATURORY AND/OR CONSTITUTION VIOLATIONS

Theft of Property (TEX. PENAL CODE § 31.03)

369. Plaintiff's iDevices are "property" under TEX. PENAL CODE § 31.01(5)(b). Personal address books, and their data therein, whether in electronic or physical media, is also "property" under TEX. PENAL CODE § 31.01(5). Plaintiffs own their respective iDevices and their personal address books maintained on their iDevices.

370. By their actions described herein, the App Defendants have unlawfully appropriated each Plaintiff's iDevice and at least a portion of their iDevice address book within the meaning of TEX. PENAL CODE §§ 31.01(4) and 31.03(b)(1). The non-consensual taking of Plaintiffs' address books and transmission to the App Defendants constitutes a "transfer [of a] . . . non-possessory interest in the [user's address book] to" the App Defendant, consumes device processing power, battery power and life, band-width, electricity and wireless and cellular airtime during the surreptitious transmissions of the address books, and causes the unauthorized disclosure and de-privatization of those materials. Plaintiffs did not effectively consent to these actions.

371. Incident to the non-consensual transmission and uploading of their address books, Plaintiffs were deprived of airtime on their iDevices and computing and processing power, resources and battery life. Plaintiffs also were deprived of control over their address book data and the data's value. Defendants have de-privatized the data and it is unlikely that any defendant will return or fully expunge from their computer systems and social networks the data, nodes and connections created therein based upon the Plaintiffs' appropriated address book materials.

372. Accordingly, each App Defendant has committed theft under TEX. PENAL CODE § 31.03 and, as applicable, under the California Penal Code. On information and belief, the

aggregate value of all address book materials acquired by each App Defendant is, in the aggregate, substantial and in excess of $200,000. Because each App Defendant's thefts are part of one scheme, the amounts also may be aggregated for violations under TEX. PENAL CODE § 31.03(e)(7).

C. TEXAS AND CALIFORNIA STATUTORY AND/OR CONSTITUTIONAL CLAIMS

1. TEXAS THEFT LIABILITY ACT (TEX. CIV. P & REM. CODE §134.001, ET SEQ

373. Plaintiffs incorporate the preceding paragraphs and further allege:

374. Each App Defendant has committed a series of thefts of property in violation of TEX. PENAL CODE § 31.03. The aggregate value of property appropriated by each App Defendant in its series of thefts is substantial.

375. Plaintiffs had a possessory interest in their identified property, which was unlawfully appropriated from them by each App Defendant.

376. Each App Defendant is liable to Plaintiffs under TEX. CIV. PRAC. & REM. CODE § 134.03.

377. Plaintiffs sustained damages as a result of the App Defendants' actions and are entitled to recover from them actual damages for each theft. *See* TEX. CIV. PRAC. & REM. CODE § 134.04. On information and belief, the actual damages should be no less than the fair market value to acquire in an arms-length transaction the property appropriated (i.e., the market value of the appropriated address book materials).

378. Under Texas' Theft Liability Act, each Plaintiff is also entitled to recover from each App Defendant who has stolen any portion of the address book from his of her respective

iDevice(s) an additional sum as determined by the trier of fact of up to $1,000 per each separate instance of theft.

2. CALIFORNIA PENAL CODE § 502

379. Plaintiffs incorporate the preceding paragraphs and further allege:

380. App Defendants violated Cal Penal Code §502(c)(2) by knowingly and without permission accessing, taking ,and using Plaintiffs' and Class Members' contact address books.

381. App Defendants copied, used, made use of, interfered with, and/or altered data belonging to Class members (1) in and from the state of California; (2) in the home states of Plaintiffs and Class members; and (3) in the states in which the servers that stored information obtained from Plaintiffs and Class Members and the websites with which they interacted were located.

382. Cal Penal Code §502(j) states: "For purposes of bringing a civil or a criminal action under this section, a person who causes, by any means, the access of a computer, computers system, or computer network in one jurisdiction from another jurisdiction is deemed to have personally accessed the computer, computer system, or computer network in each jurisdiction."

383. App Defendants have violated §502(c)(1) by knowingly and without permission altering, accessing, and making use of Plaintiffs' and Class members' contact address books on their iDevices, and using the contact information in the contact address books in order to execute a scheme to defraud consumers into registering as members of their respective Apps, and to wrongfully obtain the date in Plaintiffs' and Class members' contact address books.

384. App Developer Defendants have violated Cal. Penal Code §502(c)(2) by knowingly and without permission accessing, taking, and using Plaintiffs' and Class members' contact address book data.

385. App Defendants have violated Cal. Penal Code §502(c)(6) and §502(c)(7) by knowingly and without permission providing, or assisting in providing, a means of accessing Plaintiffs' and Class members' iDevices, in particular their contact address book data.

386. App r Defendants have violated Cal. Penal Code §502(c)(8) by knowing and without permission introducing a computer contaminant into the transactions between Plaintiffs and Class Members and the App Defendants' Apps harvesting instructions and tracing mechanisms associated with digital content. Cal. Penal Code §502(b)(10) defines "Computer Contaminant" as meaning any set of computer instructions that are designed to…. record, or transmit information within a computer, computers system, or computer network without the intent or permission of the owner of the information.

387. As a direct and proximate cause of App Defendants' unlawful conduct within the meaning of Cal. Penal Code §502, App Defendants have caused loss to Plaintiffs and the Class Members in an amount to be proven at trial. Plaintiffs and Class Members are also entitled to recover their reasonable attorneys' fees under Cal. Penal Code §502(e).

388. Plaintiffs and Class members seek compensatory damages in an amount to be proven at trial, and injunctive or other equitable relief.

389. Plaintiffs and Class members are entitled to punitive damages under Cal Penal Code §502(e)(4) because App Defendants' violations were willful, and, upon information and belief, App Defendants are guilty of oppression, fraud, or malice as defined by Cal. Civil Code §3294.

390. Plaintiffs and Class members have also suffered irreparable injury from those unauthorized acts of disclosure, to with, their personal, private, and sensitive information, including contact address book data and information on online interactions, have been harvested, viewed, accessed, stored, and used by App Defendants, and have not been destroyed, and due to the continuing threat of such injury, have no adequate remedy at law, entitling Plaintiffs and Class Members to injunctive relief.

3. THE TEXAS WIRETAP ACTS[1]

391. Plaintiffs incorporate the preceding paragraphs and further allege:.

392. Each Defendant's App constitutes an "electronic, mechanical or other device" within the meaning of TEX. CODE CRIM. PROC. art. 18.20, § 1(3) and TEX. PEN. CODE § 16.02(a).

393. The App Defendants intentionally intercepted, disclosed and/or used the contents of electronic communications containing Plaintiffs' address book materials.

394. Plaintiffs were harmed by the App Defendants' conduct allege herein, and Plaintiffs seek statutorily available damages.

4. CALIFORNIA PENAL CODE § 630 ET SEQ. CALIFORNIA WIRE TAP/INVASION OF PRIVACY ACT

395. Plaintiffs reallege the preceding paragraphs.

396. On information and belief, computer systems and servers of the following California-headquartered App Defendants ("CADs'") are located in California: Foodspotting, Hipster, Instagram, Path, Twitter and Yelp.

[1] *See also* CAL. PENAL CODE § 502(e)(1) (authorizing a civil recovery of compensatory damages for the unauthorized access, copying or use of another's computer or computer data) and § 637.2 (authorizing civil actions for each victim of eavesdropping or wire tapping under CAL. PENAL CODE §§ 631 or 632 to recover from the violator a monetary award of ***the greater of*** $5,000 or three times actual damages).

397. On information and belief, the unauthorized CAD-associated transmissions of Plaintiffs' address book materials resulted, in whole or in part, in the Plaintiffs' address book materials being electronically transmitted within California and, on information and belief, within the CADs' computer systems and outsourced systems located in California.

398. Accordingly, Plaintiffs are entitled to the benefits and protection of and the CADs are subject to California Penal Code section 631.

399. The CADs were not intended recipients of the Plaintiffs' iDevice CAD-related transmissions, which occurred without Plaintiffs' authorizations.

400. The CADs willfully and without Plaintiffs'' consent read, or attempted to read, or to learn the contents of such unauthorized address book transmissions while they were in transit over the Internet within California and being received, did learn such contents and made use of the contents of such communications, all without the consent of the Plaintiffs.

401. The CAD's accessing the address books or derivatives thereof of the Plaintiffs was without authorization and consent;

402. Communications from the CADs to Plaintiffs were sent from California. Communications from Plaintiffs' iDevices were received by the CADs and sent to California.

403. Plaintiff did not consent to any of the CAD's actions.

404. None of the CADs are a "public utility engaged in the business of providing communications services and facilities…" and the actions alleged herein by the CADs were not undertaken "for the purpose of construction, maintenance, conduct or operation of the services and facilities of the public utility."

405. The actions alleged herein by the CADs were not undertaken with respect to any telephonic communication system used for communication exclusively within a state, county, city and county, or city correctional facility.

406. The CADs directly participated in the interception, reading, and/or learning of the contents of the communications between Plaintiff, Class Members and California-based web entities.

407. Accordingly, the CADs, Defendants Foodspotting, Hipster, Instagram, Path, Twitter and Yelp, have willfully violated California Penal Code section 631.

408. Plaintiffs have suffered loss by reason of these violations, including, without limitation, violation of the right of privacy.

409. Unless restrained and enjoined, the CADs will continue to commit such acts. Under Section 637.2 of the California Penal Code, Plaintiffs have been injured by the violations of California Penal Code section 631 and are entitled to damages and injunctive relief.

D. SECONDARY LIABILITY CLAIMS

1. AIDING AND ABETTING/ASSISTING AND ENCOURAGING AS TO APPLE

410. Plaintiffs incorporate the preceding paragraphs and further allege:

411. Apple receives substantial financial, economic, advertising, public relations and other benefits from its approval, release, sale and distribution of the Apps identified in this Complaint.

412. Apple provided material support and assisted and helped in the creation, marketing and distribution of the Defendants' respective Apps as described above and by knowingly and/or recklessly permitting the surreptitious collection of Plaintiffs' address books and unauthorized operations of their iDevice.

413. Before February of 2012, Apple never individually instructed any of the App Defendants to make their Apps hash any bulk uploads of portions of user's address books or to include any address book-related user alerts or permission dialogue boxes in any of their Apps.

414. Apple's encouragement, assistance and support of each App Defendant were substantial factors leading to the above-described harms being inflicted upon the Plaintiffs and a proximate cause of Plaintiffs' damages.

2. AIDING AND ABETTING/ASSISTING AND ENCOURAGING AS TO FACEBOOK

415. On information and belief, Facebook authorized, approved and facilitated the continued distribution of the *Gowalla* App after its acquisition of *Gowalla* (and/or its personnel and technology). On information and belief, Facebook provided material support and assistance and helped in the continued production and distribution of the *Gowalla* App after its acquisition of *Gowalla* (and/or its personnel and technology). On information and belief, Facebook conducted due diligence regarding the operation and functionality of the *Gowalla* App prior to its acquisition of *Gowalla* (and/or its personnel and technology) and was aware of the *Gowalla* App's automated, non-consensual address book data harvesting functionality.

416. Accordingly, for the periods subsequent to Facebook's acquisition of Gowalla and Facebook knowingly or recklessly aided and abetted Gowalla in the commission of the wrongful activities described above and, consequently, may be both independently and/or jointly and severally liable to the Plaintiffs on each of the claims and for all of the harm and damages described herein pertaining to Gowalla during those periods.

E. EQUITABLE CLAIMS

1. UNJUST ENRICHMENT

417. Plaintiffs incorporate the preceding paragraphs and further allege:

418. The Defendants have been unjustly enriched by their wrongful actions described above.

419. On information and belief Defendants have retained the benefits and profits that they obtained and/or realized from their unauthorized acquisition, uploading, interception, remote storage and/or use of Plaintiffs' address book materials. As of yet, on information and belief, Defendants have not fully purged or disgorged their computer systems, databases and/or social networks of information, data nodes and coupled data links originally taken or gleaned from Plaintiffs' surreptitiously obtained address book materials.

420. On information and belief, the Defendants benefited from their unauthorized acquisition, uploading and use of Plaintiffs' address book materials. On information and belief, their use of the individuals' address book materials helped facilitate the rapid and exponential growth of each of their respective social networking databases and services or gaming platforms. By doing so, they further enhanced the overall economic value of each of their respective organizations and business operations for fundraising, acquisition, advertising and other purposes.

421. On information and belief, the Defendants and Apple have also received revenues and other benefits associated with their distribution and/or sales of the non-conforming malicious Apps identified herein.

422. As a result of the Defendants' wrongful conduct described herein, each Defendant has received, directly or indirectly, funds and other valuable benefits which each company was not rightfully or equitably entitled to in an amount to be determined at trial, and has been unjustly enriched thereby.

2. CONSTRUCTIVE TRUST

423. Plaintiffs incorporate the preceding paragraphs and further allege:

424. On information and belief, the Defendants have inequitably profited from their wrongful activities described herein and have been unjustly enriched by their wrongful actions described above.

425. To protect Plaintiffs' rightful interests, Plaintiffs are entitled to and the Defendants' actions necessitate the imposition of a constructive trust over all funds and benefits (or the proceeds thereof) either: (a) wrongfully received or obtained by the Defendants in connection with or derived from either, (i) their wrongful access, upload, interception and/or use of Plaintiffs' address book materials and/or iDevices, or (ii) the sale or distribution of the non-conforming Apps, or (b) on account of their other wrongful activities described herein.

426. To prevent further immediate and irreparable harm, the Court should immediately enjoin any disposition by Defendants of any such funds or valuable benefits.

427. On information and belief, the value of social networking companies—including Foursquare Labs, Path, Gowalla, Instagram, Foodspotting, Yelp – is based upon and roughly proportional to their user base or the overall size and connectedness of their respective networking databases. Thus, the defendants' own business value has been enhanced by the nonconsensual use, inclusion and linkage of Plaintiffs' address book materials in the defendants' operational social networking databases and, on information and belief, has accelerated and helped facilitate the exponential growth of the defendants' networks and businesses.

428. Accordingly, to protect Plaintiffs' rightful interests and to prevent the unjust and inequitable enrichment of the defendants, the Defendants' actions necessitate the imposition of a constructive trust over: (i) a percentage to be determined at trial of each App Defendant's outstanding equity on a fully-diluted basis and any proceeds from any sale thereof; (ii) a

percentage to be determined at trial of the gross proceeds received or promised on any sale or disposition of the equity or operational business segment of any App Defendant; and (iii) any Gowalla assets, or the proceeds thereof, distributed to any Gowalla equity holders, officer or directors for less than fair value or in violation of the provisions of the Uniform Fraudulent Transfer Act.

429. To protect consumers' privacy and to prevent further immediate and irreparable harm to the Plaintiffs, to the Class members and to wireless mobile device consumers as a whole, the Plaintiffs ask the Court to: (a) direct Apple to actually enforce against all App developers the user-data-privacy provisions contained in Apple's App development agreements and policies; and (b) enjoin Apple from initiating any further downloads to others of Apps (including those identified herein) that: (i) transmit and/or upload in unencrypted or un-hashed form any bulk portion(s) of their App users' address book, or (ii) have data-uploading functionality and access any portion of the App users' address book in advance of an alert, appropriate notification regarding the planned use of the data, and the confirmation of explicit permission to do so from the device owner.

3. DECLARATORY JUDGMENT

430. Plaintiffs reallege the above paragraphs.

431. Apple has contended that Plaintiffs are subject to enforceable agreement(s) with Apple that, according to Apple, limit Plaintiffs' rights to ordinary consumer protections and to seek judicial relief in a forum of their choosing and that supplant customary consumer rights and remedies provided by law and statute on matters pertaining to harmful acts committed by Apple and harms caused, in part, by Apps and iDevices made, marketed and sold by Apple.

432. Plaintiffs dispute that any such valid or enforceable agreement(s) exists. On information and belief, any such purported term(s) or agreement(s) are, *inter alia*, illusory, unenforceable, unconscionable, contrary to public policy, or simply inapplicable.

433. Thus, a real, present, substantial and concrete justiciable controversy exists between Plaintiffs and Apple regarding the existence, validity, enforceability and applicability of any such term(s) or agreement(s)

434. Accordingly Plaintiffs are entitled under 18 U.S.C. § 2201 to a declaration adjudicating the existence, validity, enforceability and applicability of any such term(s) or agreement(s) as well as the parties' respective rights and responsibilities thereunder, should there be any.

435. Plaintiffs also ask the Court to declare any such purported term(s) or agreement(s), in whole or in part, invalid, unconscionable, unenforceable and/or void, *in abnitio.*

E. RELIEF

1. INJUNCTIVE RELIEF.

436. Plaintiffs have no adequate remedy at law and, on information and belief, the Defendants' wrongful conduct will continue in whole or in part, unless enjoined by this Court. Plaintiffs are entitled as alleged herein to immediate, temporary, preliminary and permanent injunctive relief, including the following:

> (i) an order prohibiting the distribution or operation of Apps having coding and/or functionalities that can or do cause either: (A) the unhashed or unencrypted upload of any bulk portion of an iDevice owner's address book materials, and (B) the upload of any such address book materials prior to an alert and the owner granting explicit, knowing permission for the upload and any subsequent use of such materials;
>
> (ii) an order prohibiting any continued non-authorized use of Plaintiffs' address book materials and requiring the return and/or deletion from Defendants' computers and computer systems—as verified by an independent third party data security company—of

any wrongfully obtained portions of Plaintiffs' address book materials as well as any data, data nodes or data connections derived therefrom;

(iii) an order requiring Defendants to submit to periodic compliance audits by an independent, third-party data security company regarding the privacy and security of iDevice users' address book materials and the handling of any such materials that may come into Defendants' possession, custody or control;

(iv) an order enjoining Defendants' violations of any of the criminal laws cited herein;

(v) an order mandating that Apple: (a) provide iDevice users with a built-in option for the encrypted storage of their address book on their iDevices, and (b) require hashing of any automatic or bulk uploads of user address book materials for purported matching purposes; and,

(vi) an order directing the Defendants to preserve and maintain throughout the course of this proceeding all evidence pertaining to this matter—including computer and electronic records, historical App code, and records relating to attempts to access the iDevice of any Plaintiff or to subsequently upload, copy, use, store, or disseminate any portion of any Plaintiff's address book materials.

All conditions precedent to Plaintiffs' claims for relief have been performed and/or occurred.

437. **EQUITABLE RELIEF.** To prevent the unjust enrichment of the Defendants, Plaintiffs are also entitled to equitable relief, including an award of and/or the imposition of a constructive trust over (i) any profits or benefits Defendants received, obtained or realized from their wrongful access or unauthorized use of Plaintiffs' iDevices and/or acquisition or use of any portion of their address books; and (ii) to compensate for the unwarranted accelerated growth of certain Defendants' social networks, user base and overall business via the use of portions of Plaintiffs' and the Class members' address books, a percentage to be determined at trial of (a) each such defendant's and Defendant's outstanding equity on a fully-diluted basis and any proceeds from any sale thereof; and (b) the gross proceeds received or promised on any sale or disposition of the equity or operational business segment of any such Defendant.

PRAYER

438. Plaintiffs, on behalf of themselves and the Class members, further request that upon final trial or hearing, judgment be awarded against Defendants, in favor of Plaintiffs and the Class members, for (as described above):

(i) actual, compensatory, incidental, consequential, statutory, and/or nominal damages and an award of Defendants' wrongfully obtained profits;

(ii) statutory treble damages;

(iii) exemplary and punitive damages (as described above and as statutorily authorized);

(iv) injunctive relief as set forth above;

(v) imposition of constructive trusts as described herein and disgorgement of any benefits wrongfully received or obtained by the Defendants;

(vi) declaratory relief asset for the above

(vii) pre- and post-judgment interest at the highest applicable legal rates;

(ix) attorneys' fees and litigation expenses incurred through trial and any appeals;

(x) costs of suit;

(xi) an order under 11 U.S.C.S. § 523(a)(6) that Defendants be prohibited from any discharge under 11 U.S.C.S. § 727 for injuries caused to Plaintiffs' and the Class members by Defendants' malicious and willful conduct, and,

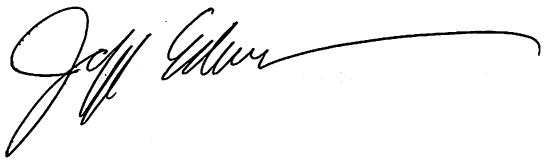
(xii) such other and further relief that this Court deems just and proper.

JURY DEMAND

439. Plaintiffs request a jury trial on all issues triable in this action.

Respectfully submitted,

EDWARDS LAW



By: _____

Jeff Edwards
State Bar No. 24014406
THE BREMOND HOUSTON HOUSE
706 GUADALUPE
Austin, Texas 78701
Tel. 512-623-7727
Fax. 512-623-7729
jeff@edwards-law.com

Carl F. Schwenker
Texas Bar No. 00788374
LAW OFFICES OF CARL F. SCHWENKER
The Bremond-Houston House
706 Guadalupe Street
Austin, Texas 78701
Tel. (512) 480-8427
Fax (512) 857-1294
cfslaw@swbell.net

Dirk Jordan
Texas Bar No. 00784359
Jordan Law Firm
The Bremond-Houston House
706 Guadalupe Street
Austin, Texas 78701
512-551-0669
512-551-0668 fax
dirk@dirkjordan.com

ATTORNEYS FOR THE PLAINTIFFS
AND THE PUTATIVE CLASS